UNDERSTANDING RUSSIAN OFFENSIVE CYBER TO REPAIR PRIVATE-PUBLIC RELATIONS IN CRITICAL INFRASTRUCTURE DEFENSE

by
Christopher M. Yee-Paulson

A research study submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
December 2020

Abstract

This policy study assesses how concepts of monitoring IT (Information Technology) and OT (Operational Technology) mitigate the success of Russian Offensive Cyber Operations (OCO) against critical infrastructure. The study answers, "how can monitoring systems that surveil both IT and OT mitigate offensive Russian cyber operations against critical infrastructure?" Current scholarship shows substantial efforts to reform cyber defenses – exemplified by the US's changes since the early 2000s. Although reforms resulted in new defensive programs, they contributed to a convoluted system that made private-public cooperation difficult. Combined with technological trends that emphasized cost-efficiencies, these reforms created a contentious balance between private and public organizations where infrastructure providers valued costs over security. This unfortunate position supports Russia's strategy. Russian cyber-attacks since 2007 illustrate increasingly destructive capabilities that manipulate critical infrastructure vulnerabilities and weak defenses.

This study examines Russian cyber-attacks since 2007 to test if Moscow's cyber tactics create abnormal behavioral traits that modern surveillance, IT-OT monitoring, could detect. Through comparative case studies of Russian OCO, the study builds common TTPs (Tactics, Techniques, and Procedures) and possible warning signs. The results are the foundation of several policy recommendations. The study used data from established technical trade associates, non-governmental organizations, government agencies, translated Russian strategy documents, and scholarly literature that discussed Russia's cyber activities.

The analysis indicates that Russia's offensive cyber creates several observable behavioral traits that IT-OT monitoring would detect, mitigating Russian OCO's success

against critical infrastructure. However, the technique needs to intervene when an attacker is in initial set-up phases, as the beginning segments of a Russian OCO are the most vulnerable to detection. The study recommends streamlining government cybersecurity and regulatory agencies, providing the necessary intelligence to customize defensive systems, and broadening access to commercial solutions. These steps would help create a collaborative relationship between the public and private sector while encouraging the broad adoption of IT-OT monitoring. The study concludes that the government should focus on policies that support industry to encourage cybersecurity modernization and avoid problems seen in America's reforms during the 2000s.

Primary Reader and Advisor: Professor Sarah Clark

Secondary Readers: Professor Michael Warner and Professor Mark Young

Preface and Acknowledgments

I would like to thank my wife, Icy Li, for her patience and steadfast support through my participation in the Johns Hopkins Global Security Studies program, as her encouragement kept me motivated in the most challenging times. I would like to thank my parents for their encouragement and constant willingness to provide feedback on my ideas. Thank you to my fellow students, professors, colleagues, and friends who helped me during this research study and supported the long journey to pursue higher education.

Table of Contents

List of Figures and Tables

Introduction: Russian Offensive Cyber and Critical Infrastructure Reforms

Modern cyber-attacks are technically complex and can inflict physical damage, making the security of critical infrastructure vital. Russia is one of the primary threats for offensive cyber, and it has a history of targeting critical infrastructure dating back to the late 1990s. US cybersecurity reforms in the 2000s noted that early Russian cyber aggression could lead to attacking critical infrastructure. While new agencies, authorities, and defensive programs tried to address various cyber threats, they helped create a culture where private organizations focus on costs over security because of confusing federal processes and authorities. These trends became compounded by technological movements that focused on automation and streamlining security. As the Russian cyber threat evolves, detailed research surrounding modern cybersecurity is crucial to providing policymakers with actionable recommendations on changing private-public cybersecurity relationships while learning from past mistakes.

This policy study aims to answer the following research question: "how can monitoring systems that surveil IT (Information Technology) and OT (Operational Technology) mitigate offensive Russian cyber operations against critical infrastructure?" Answering this question requires an in-depth study of modern Russian cyber-attacks to determine a standard set of tactics that Moscow typically leverages against critical infrastructure. These common characteristics are necessary to see if they create abnormal behavioral cyber traits that threat-informed surveillance, such as IT-OT monitoring, can detect – thus, mitigating Russian OCO success rates. This study aims to create policy recommendations for defending critical infrastructure by looking at literature about Russian cyber capabilities and cybersecurity scholarship.

Common Definitions to Frame the Policy Study

Critical Infrastructure

Typically, election-related components are not part of critical infrastructure definitions – DHS (Department of Homeland Security) does not include this component.[1] However, the scope and breadth of Russian cyber operations against the US Presidential election in 2016 warrants adding this element. Therefore, this study defines critical infrastructure as vital physical, cyber, or technological assets that contribute to a country's operation and whose incapacitation would debilitate economic, political, or public safety.[2,3,4]

Offensive Cyber Operation (OCO)

Offensive Cyber Operation's definition stems from the US military's doctrine written by the Joint Chiefs of Staff and Russian strategy from Moscow's Ministry of Defense. The study's definition focuses on offensive or destructive acts in cyberspace. This study defines OCO as a destructive computer network activity that deliberately

---

[1] DHS.gov. "Critical Infrastructure Security." Department of Homeland Security. https://www.dhs.gov/topic/critical-infrastructure-security.
[2] Eric Manpearl. "Securing US Election Systems: Designating US Election Systems as Critical Infrastructure and Instituting Election Security Reforms." *BU Journal of Science. & Technology. L.* 24 (2018): p. 168-169. https://www.bu.edu/jostl/files/2018/03/5-Manpearl-Online-Version.pdf
[3]Arjen Boin and Allan McConnell. "Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience." *Journal of Contingencies and Crisis Management* 15, no. 1 (2007): p. 50-51. http://www.academia.edu/download/39525042/Preparing_for_Critical_Infrastructure_Br20151029-30676-1u12me.pdf
[4] DHS, "Critical Infrastructure Security"

causes harmful effects against a technology-related target, critical infrastructure, or associated supporting components using technical means.[5,6,7]

Information Technology (IT) and Operational Technology (OT)

One of the leading associations on cybersecurity for infrastructure, the SANS Institute, defines IT as a broader set of systems that processes, stores, or transmits data – a corporate intra-network, for example. The SANS Institute defines OT as hardware or software that manages physical equipment. For example, these can include power controls and safety systems.[8]

IT-OT Monitoring

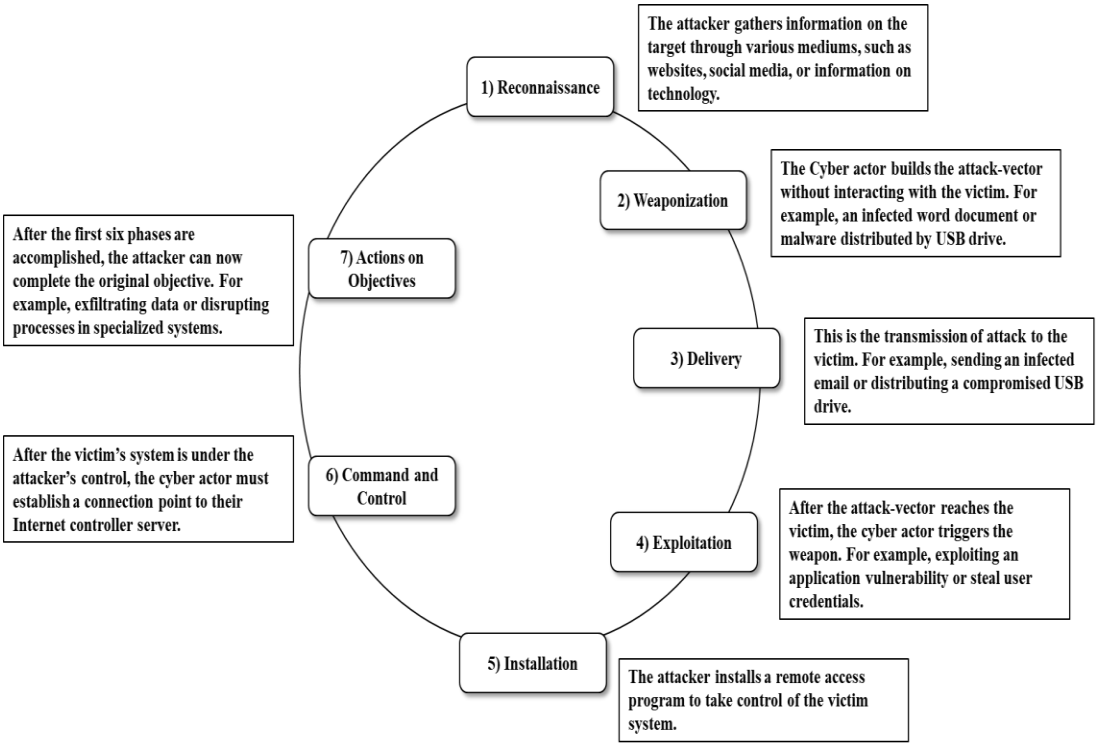
According to Knapp, Langill, and DHS, IT-OT monitoring – sometimes referred to as advanced persistent diligence – relies on the concept of defense-in-depth, which calls for monitoring across multiple network layers.[9,10] The surveillance requires "detecting and alerting an organization of an intrusion early on so they (the organization) can take defensive action before critical assets are breached."[11] By relying on anomaly

---

[5] "Cyberspace Operations." Joint Publication 3-12. Joint Chiefs of Staff, June 8, 2019. p. 1-13, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.
[6] James E. Cartwright (General, VCJCS). "Joint Terminology for Cyberspace Operations." Memorandum for Chiefs of The Military Services Commanders of The Combatant Commands Directors of The Joint Staff Directorates. Washington, D.C.: Joint Chiefs of Staff, November 2010. p. 1-3, https://www.hsdl.org/?abstract&did=734860.
[7] Ministry of Defense of the Russian Federation. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space) (Moscow, 2011). p. 1-3. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle
[8] Derek R. Harp and Bengt Gregory-Brown. "IT/OT Convergence: Bridging the Divide." White Paper. The SANS Institute and Nex Defense, 2014. p. 1-3, https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf.
[9] "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies." ICS-CERT White Paper. Washington, D.C.: Department of Homeland Security, September 2016. p. 27, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf?force_isolation=true.
[10] Eric D. Knapp, and Joel Thomas Langill. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and other Industrial Control Systems*. Syngress, 2014. p. 30-36; 50-53.
[11] DHS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 27

detection logic, IT-OT monitoring specifically looks for observable intrusion behaviors to alert defenders of possible attacks. These are actions outside what an authorized user would conduct in their daily duties that indicate possible malicious intentions.[12]

Figure 1: Cyber Kill Chain Details[13,14]



Cyber Kill Chain

The cyber kill chain is a series of standard phases that are common to most computer network attacks. For cyber intrusions, the goal is to develop an attack vector, breach the target, establish a presence, and deliver a desired action on the objective. Based on these goals, a generalized cyber kill chain has the following characteristics:

[12] Ibid, 15-32
[13] Ibid
[14] Hutchins et al. 3-5

reconnaissance, weaponization, delivery, exploitation, installation, Command and Control (C2), and actions on objectives.[15,16]

Policy Issue Background: The Russian Cyber Threat and Troubled Reforms

In the 2000s, America passed several cybersecurity reforms in response to rising state-supported cyber threats. Unfortunately, the policies created a disjointed set of policies.[17] Reforms like Presidential Policy Directive (PPD) 7, the Energy Policy Act, establishing the National Cybersecurity and Communications Integration Center (NCCIC), and creating the National Infrastructure Protection Plan (NIPP) were a cornerstone of America's cyber defenses.[18,19] Although these policies created a sizeable federal cybersecurity apparatus, the changes contributed to confusing initiatives that separated cyber defense and regulatory authorities – which hurt collaboration with private industry – according to the Congressional Research Service.[20]

The study reviews US reform efforts as an example of problematic policy approaches to cybersecurity because of greater data availability. However, current scholarship indicates that other Western-aligned nations experienced similar fragmented private-public relationships resulting from government-focused cybersecurity

---

[15]Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." Lockheed Martin Corporation, January 2011. p. 3-5. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[16] Spitzner, Lance. "Applying Security Awareness to the Cyber Kill Chain." SANS Institute, May 31, 2019. p. 1-5. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain.

[17] Paul Parfomak, Richard Campbell, and Chris Jaikaran. "Cybersecurity for Energy Delivery Systems: DOE Programs." CRS Report. Congressional Research Service, August 28, 2017. p. 17-20, https://crsreports.congress.gov/product/pdf/R/R44939.

[18] Parfomak et al. 4-9; 17-20

[19] "Preventing and Defending Against Cyber Attacks." Washington, DC: Department of Homeland Security, June 2011. p. 1-3. https://www.dhs.gov/xlibrary/assets/preventing-and-defending-against-cyber-attacks.pdf.

[20] Parfomak et al. 4-9; 17-20

reforms.[21,22] Combining cyber behavioral warning signs exhibited by Russian OCO that modern defensive techniques, IT-OT monitoring, can detect with policy lessons learned from the 2000s are crucial to a more successful private-public cybersecurity relationship.

An interdisciplinary methodology that also leverages an understanding of Russia's approach to offensive cyber would enable policy-relevant conclusions to improve the adoption of modern cybersecurity techniques. Russia maintains a destructive view of offensive cyber, and its harmful actions since at least the 1990s demonstrate a pressing threat. It is vital to comprehend how an adversary thinks about the strategic, operational, and tactical application of a capability while examining why current policy approaches are problematic.

Framing the Threat: Russian OCO Uses the Online Domain to Cripple Adversaries

Russia's use of cyberspace originates in the late 1990s.[23] During the Moonlight Maze campaign of 1999, Russian hackers stole data from the DoD (Department of Defense), DoE (Department of Energy), NASA (National Aeronautics and Space Administration), and several military contractors. The Moonlight Maze operation became one of the first known Russian cyber operations and highlighted potential defensive vulnerabilities in America. Russia's capabilities began a dialogue, starting in the US,

[21] Madeline Carr. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): p. 43-62. https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

[22] Myriam Dunn-Cavelty and Manuel Suter, 'Public–private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection,' *International Journal of Critical Infrastructure Protection* 2: 4, 2009, p. 181-190

[23] Russian cyber programs have roots in the 1950s when cybernetic programs helped build Soviet machine communication projects as the foundation for future online capabilities. However, this study considers the 1999 Moonlight Maze operation the first modern Russian OCO because it leveraged early IT networks to steal data from multiple organizations – attributes not present in older Soviet programs. See Slava Gerovitch's *From Newspeak to Cyberspeak*.

about Moscow's ability to target critical infrastructure – helping to start monitoring programs in several public and private sectors.[24]

Since 1999, Russia gradually built an integrated approach to offensive cyber that focused on information dominance to degrade the adversary – a strategy well suited to manipulate fragmented policy approaches to cybersecurity. As Moscow's cyber capabilities evolved, OCO became a viable method for leveraging tactics that operate below the armed conflict level while still damaging adversarial infrastructure. By 2007, Russian offensive cyber tactics evolved from data theft to damaging critical infrastructure. Russia's DDoS (Distributed Denial of Service) attack against Estonia in April and May of 2007 represented a concerted effort to take advantage of its interconnected online systems to slow communications and shutdown key financial institutions.[25] Unlike the Moonlight Maze operation in 1999, Connell and Vogler note that the Estonia operation was a deliberate attack that fomented fear in the population and focused on taking advantage of a public-private system that valued online efficiency.[26]

By 2015, Russian OCO against critical infrastructure evolved significantly, resulting in the first malware-based cyber-attack against another nation's electrical grid. The operation shut down Ukraine's power for over 220,000 people.[27] In 2016, Russian cyber actors launched considerable efforts to target the US Presidential election. A prominent component was the hacking operations against US political parties aimed at disrupting the electoral process, according to the Office of the Director of National

[24] Shackelford et al. 322-30

[25] Michael Connell and Sarah Vogler. "Russia's Approach to Cyber Warfare." Center for Naval Analyses, March 2017. p. 13, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.
[26] Ibid, 13-16
[27] Ibid, 16-22

Intelligence.[28] The 2016 cyber operations against America was part of a gradual Russian capability buildup designed to target a wide range of critical infrastructure and manipulate defensive vulnerabilities.[29]

Russia's approach to the online domain highlights why OCO (Offensive Cyber Operations) is a vital part of its approach and enables manipulating critical infrastructure weaknesses. However, understanding Russian offensive cyber means distinguishing it from information warfare. During the 2016 US Presidential elections, the distinction was apparent when Russia used online disinformation and malicious hacking. Connell, Vogler, and Giles highlight that Russian offensive cyber is a subset of information warfare designed to enable more destructive tactics that degrades an adversary. Although Russian offensive cyber is related to information warfare strategically, it remains a separate function because it uses specific technical means.[30,31] According to Giles and General Valery Gerasimov – Chief of the Russian General Staff – Russia's approach to information warfare traces back to the Soviet era and broadly includes asymmetric tactics like information operations, disinformation campaigns, and more recently, cyber-attacks.[32,33] Further Russian scholarship aligns with this view, indicating that information

[28] "Assessing Russian Activities and Intentions in Recent US Elections." Intelligence Community Assessment. Office of the Director of National Intelligence, January 6, 2017. p. 1-3, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[29] ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," 2
[30] Connell and Vogler, 3
[31] Keir Giles. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," March 21, 2016. p. 9; 61-64 https://www.chathamhouse.org/publication/russias-new-tools-confronting-west.
[32] Ibid, 11
[33] Gerasimov, 25

warfare, and the specialized destructive subcomponent of offensive cyber, focus on information dominance without force.[34]

Russia's broad understanding of information warfare enables it to use damaging cyber capabilities more flexibly because Moscow considers cyberspace a component of the information space rather than a new domain.[35,36] Gerasimov even notes that "the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy."[37] Russia's flexibility is evident in a Kremlin strategy that focuses on the Armed Forces' operations in the information domain. The strategy highlights that cyberspace is part of the information space and linked with IT, software, or supporting infrastructure to enable offensive technical tactics – such as cyber-attacks.[38] The ability to view cyberspace as an interconnected web of supporting pieces enables complex Russian cyber operations like those seen in 2016 that used offensive hacking tactics. Russia's approach works particularly well when a cyber-attack requires manipulating critical infrastructure vulnerabilities. It aligns with Moscow's view that cyber targets are a combination of virtual and physical components. Although Russian offensive cyber is a specialized subset of information warfare capabilities, destructive operations are becoming a high-tech enhancement for Russia's broader strategic approach to information

[34] Sergey Chekinov and S. A. Bogdanov. 'The Nature and Content of a New-Generation War,' Military Thought, No. 4, 2013., p. 16. https://www.semanticscholar.org/paper/The-Nature-and-Content-of-a-New-Generation-War-Chekinov-Bogdanov/c8874593b1860de12fa40dadcae8e96861de8ebd
[35] Connell and Vogler, 3-5
[36] Giles, 61-64
[37] Gerasimov, 26
[38] Ministry of Defense of the Russian Federation, "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space," p. 1-3

dominance. Destructive cyber operations remain connected to the information domain by sharing the goal of degrading the adversary with non-kinetic tactics.[39,40,41]

Understanding Russian offensive cyber strategy is crucial because it highlights a desire to degrade adversarial control of the information space by manipulating defensive weaknesses, whether technical or policy-related. The context of Moscow's strategy is crucial when analyzing approaches that countries, such as the US, created for responding to state-sponsored cyber threats. The scholarship illustrates broad offensive tactics but does not highlight if Moscow's tactics create signatures that threat-informed surveillance can detect. Understanding this level of detail is vital when evaluating whether threat-informed surveillance techniques – such as IT-OT monitoring – can mitigate Russian offensive cyber tactics. While Knapp, Langill, and DHS, broadly agree that IT-OT monitoring is promising because it can monitor all network layers and automatically detect intrusion traits, understanding specific Russian cyber behavior is crucial to corroborating efficacy against Moscow.[42,43]

The Limitations of US Cybersecurity Reforms: Problems with Modern Policy

Throughout the 2000s, America created reforms that focused on sprawling government-led cybersecurity programs as lessons from Russia's efforts in the 1990s forced policymakers to realize cyberspace's growing vulnerabilities. These policies focused on protecting critical infrastructure from nations like Russia; however, the

[39] Connell and Vogler, 1-5; 27-29
[40] Giles, 1-10; 61-64
[41] Chekinov and Bogdanov, 14-16
[42] Knapp and Langill, 30-36; 50-53.
[43] DHS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 15-32

implementation created a confusing bureaucracy.[44,45] Unfortunately, US cybersecurity reforms pushed firms to focus on costs and streamlining processes over cyber defenses because of the government's increasing requirements.

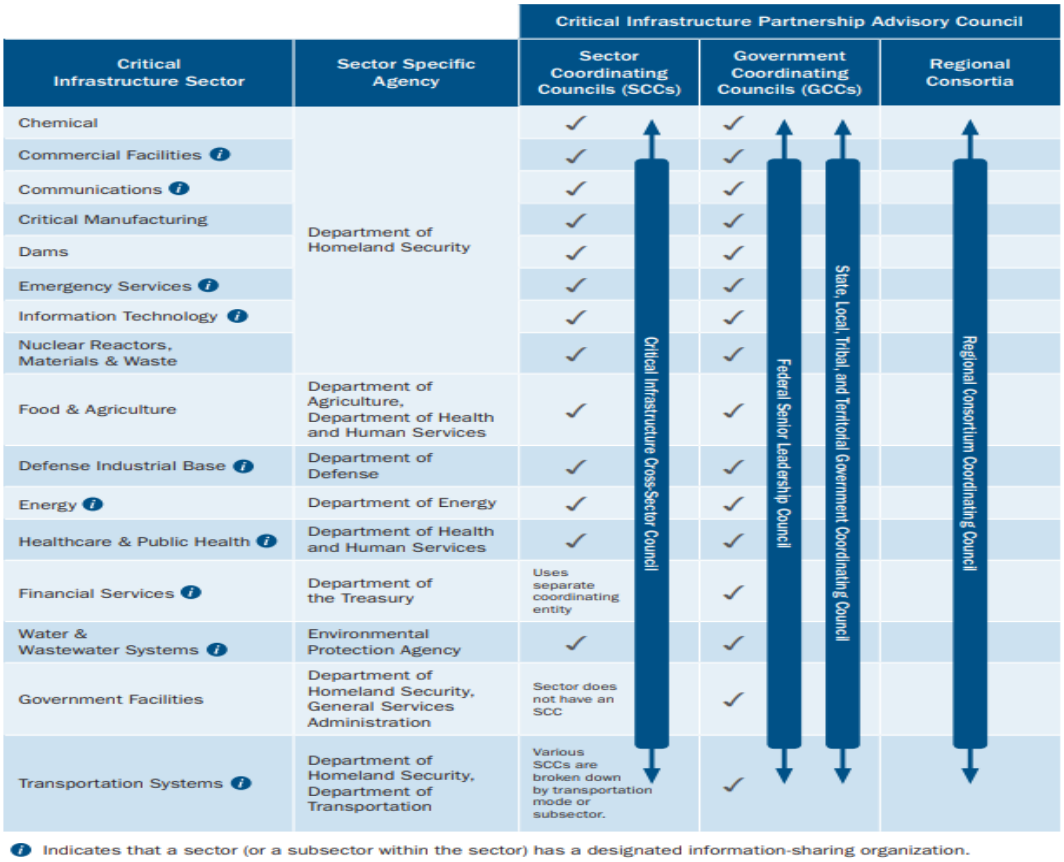
For example, in the US energy industry, the Department of Energy (DOE) and the Federal Energy Regulatory Commission (FERC) are the two-primary regulatory agencies for enforcing cybersecurity standards, according to 2003's PPD 7 and 2005's Energy Policy Act.[46] These policies would suggest that the DOE and FERC oversee cyber defenses for the energy industry. However, regulatory agencies must also coordinate with DHS because it manages the NCCIC and responds to cyber incidents – unlike regulatory bodies that focus on standards enforcement. The divide between DHS and regulatory bodies means cybersecurity responsibilities belong to multiple agencies.[47] Private firms must contend with several sets of compliance standards and coordinate with multiple federal cybersecurity agencies.

DHS attempted to improve private-public integration between 2009 and 2015 with the NIPP (National Infrastructure Protection Plan), EINSTEIN 2, and EINSTEIN 3 Accelerated – EINSTEIN 1 was a limited iteration that started in 2003.[48] EINSTEIN 2 began in 2009 and focused on a series of integrated sensors across federal infrastructure that monitored possible cyber intrusions. EINSTEIN 3 Accelerated expanded these

[44] "Preventing and Defending Against Cyber Attacks," DHS, p. 1-5
[45] Parfomak et al. 4-9; 17-20
[46] Ibid
[47] "Preventing and Defending Against Cyber Attacks," DHS, p. 1-5
[48] In 2012, DHS also established the Continuous Diagnostic Mitigation (CDM) program, which deployed a series of sensors and data integration dashboards across US civilian agencies to aide identity, network, and data management. However, CDM focuses on the .gov domain, which is why this study focuses on the EINSTEIN program that eventually expanded to private industry. See *CDM Program Overview* and appendix 1.

sensors to major private internet service providers in 2012, using classified information to detect large cyber threats signatures.[49]

Table 1: NIPP Sector and Cross-Sector Coordinating Structures[50]



Mirroring the definition of IT-OT monitoring because of its sensors across multiple networks, DHS notes that EINSTEIN provides defenders with the capability to stop an average of 5.4 million intrusions per year – each corresponding to signatures of known cyber threats.[51] While the technical capabilities of this system are not in question, implementation faced resistance. Compatibility issues, cost, authority confusion, and

[49] "EINSTEIN | CISA." Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/einstein.
[50] "National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience." Washington, DC: Department of Homeland Security, 2013. p. 10-11 https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.
[51] "Preventing and Defending Against Cyber Attacks," DHS, p. 1-3

recalcitrant civilian agencies made EINSTEIN problematic as it struggled to integrate across disparate networks. EINSTEIN is a reminder that cutting down coordination needs and streamlining implementation practices are highly impactful for adoption rates.[52,53,54]

Initially, DHS focused on defending government systems; however, the 2013 NIPP, the National Cybersecurity Protection Act of 2014, and the Cybersecurity Act of 2015 allowed the department to respond to civilian incidents. These policy efforts expanded DHS authorities and attempted to build a collaborative structure with the private sector. Table 1 illustrates how the NIPP uses coordinating councils between industry and government to improve critical infrastructure defenses. The NIPP complemented executive order 13,636 in 2013, which created a new analytical cybersecurity framework from the National Institute of Standards and Technology (NIST) – formalized into law in 2014 and updated in 2018. The new program focused on having participating organizations follow a series of guidelines, standards, and common cybersecurity practices to "identify, assess, and manage cyber risks."[55] Although the NIST methodology mostly targeted government agencies and critical infrastructure providers, it represented a significant attempt at a standard approach to cybersecurity reporting for both public and private organizations in America.[56,57]

Unfortunately, the civilian sector was still mostly responsible for defending itself. Even with increased authorities, DHS was in a more reactionary role because it could not

---

[52] Charlotte Clément-Cottuz. "Risks in Governmental Cybersecurity Program : Case Study of the Einstein Project | Journal of Strategic Threat Intelligence." *Journal of Strategic Threat Intelligence* 1, no. 37 (November 2017): 1–3.
[53] Dunn-Cavelty and Suter, 181-190
[54] Carr, 42-61
[55] "Framework for Improving Critical Infrastructure Cybersecurity." Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018. p. iv
[56] Ibid, iv
[57] Shackelford et al. 328-29

proactively intervene in civilian networks without a cyber incident occurring due to privacy regulations.[58,59] Policies like the NIPP coordinating councils and the NIST framework helped with some of the legal restrictions by building private-public collaboration points and a standard approach to cyber-threat reporting. [60,61,62] However, government cybersecurity oversight continued to grow, and despite some policy successes, private-sector firms saw an increasing number of agencies and regulations. According to the Congressional Research Service and Etizoni, America's push to increase its public cybersecurity posture helped decrease coordination with the government to avoid added costs, perceived over-regulation, and privacy violations.[63,64,65,66]

A critical technology trend that bolstered these problems was IT-OT convergence. The SANS Institute noted that IT and OT systems that were once separate are converging in critical infrastructure industries since at least the early 2000s. IT-OT convergence was born out of a desire to lower operational costs and maximize new automation technology to manage more OT with less IT.[67] These technologies were separate because connecting IT and OT requires broad access. When critical infrastructure and OT components

---

[58] Chris Jaikaran. "DHS's Cybersecurity Mission – An Overview." CRS Report. Congressional Research Service, December 19, 2018. p. 1-2 https://fas.org/sgp/crs/homesec/IF10683.pdf.
[59] "National Cyber Strategy." Washington, DC: The White House, September 2018. P. 8-11 https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[60] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 1-11
[61] "NIPP: Partnering for Critical Infrastructure Security and Resilience," DHS, 1-20
[62] The 2018 Cybersecurity and Infrastructure Security Agency Act established the Cybersecurity and Infrastructure Security Agency as the primary coordinating body responsible for critical infrastructure defense. It also absorbed responsibility maintaining the NIPP and NIST framework. See *Supporting Policy and Doctrine | CISA*.
[63] Amitai Etzioni. "Cybersecurity in the Private Sector." Issues in Science and Technology 28, no. 1 (2011): 58–61. https://doi.org/https://www.jstor.org/stable/43315569.
[64] Parfomak et al. 17-20
[65] Jaikaran, 1-2
[66] Parfomak et al. 1-10
[67] Harp and Gregory-Brown, 8-9

become remotely managed by IT, cyber actors have more attack vectors because of the increased connectivity.[68] While cybersecurity has matured, the exponential number of available attack avenues makes it difficult for network defenders to patch all vulnerabilities.[69]

Unfortunately, IT-OT convergence's push for automation causes firms to focus on cost over security by relying on new technology that can seemingly manage more tasks with fewer resources, amplifying reform problems in the 2000s. A culture of efficiency and cost reduction magnifies perceived issues with government cybersecurity oversight, driving firms to decrease public partnerships to avoid added regulatory expenses. Etizoni and the US Computer Emergency Readiness Team highlight that many critical infrastructure firms attempt to hide cyber breaches or forgo advanced defense systems to prevent public exposure and lower profits while maintaining cost efficiencies from IT-OT convergence.[70,71] The apprehension for more robust cybersecurity or cooperation with government entities comes from the fear that the new defenses or regulations will reduce network speeds, increase maintenance costs, and invite public criticism for invading privacy.[72,73] Knapp and Langill note that these concerns recognize business needs; however, they do not consider the growing capabilities of state-supported cyber actors that take advantage of the networked IT-OT architecture.[74]

---

[68] "Heightened DDoS Threat Posed by Mirai and Other Botnets." Technical Alert. Washington, DC: Cybersecurity & Infrastructure Security Agency, October 14, 2016. https://us-cert.cisa.gov/ncas/alerts/TA16-288A.
[69] Ibid, 4-5
[70] Etizoni, 58-61
[71] Parfomak et al. 17-20
[72] DHS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 29
[73] Knapp and Langill, 51-53.
[74] Ibid

As complicated cybersecurity reforms in the US progressed from 2003 to 2018, the trend of IT-OT convergence spread throughout private industry. Carr, Dunn-Cavelty, and Suter confirm that the US experience is not a localized example. Similar private-public relationship issues appeared in nations, such as the UK, Canada, and Australia, that attempted government-led reforms. However, this study focuses on the US case because of greater data availability.[75,76] Since the private sector is crucial for infrastructure management in America and other Western-aligned nations, uncooperative relationships with the government breeds weak cybersecurity practices that allow aggressive nations, such as Russia, to leverage its destructive cyber capabilities.

Organizations with lackluster cybersecurity systems or standards benefit nations like Russia and give them flexibility when operating in cyberspace. Russia's focus on destructive technical methods to achieve information dominance and degrade an adversary's infrastructure incentivizes Moscow to manipulate political and technical weaknesses.[77] A disaggregated policy approach to cyber defenses supports Russia's strategy because critical infrastructure providers are less likely to report cybersecurity problems or implement threat surveillance, such as IT-OT monitoring. Therefore, it is crucial to understand if Russian tactics exhibit observable behaviors that allow modern defensive techniques like IT-OT monitoring to intervene and build recommendations that learn from American reform problems during the 2000s to improve the adoption of threat-informed surveillance.

[75] Carr, 43-61
[76] Dunn-Cavelty and Suter, 181-190
[77] Stephen Blank. "Cyber War and Information War à La Russe." In Understanding Cyber Conflict: 14 Analogies, p. 91–93. Georgetown University Press, 2017.

Adding Value: Identifying Gaps in Modern Scholarship

One of the primary gaps in current research is the lack of nation-specific studies that confirm the effectiveness of modern cybersecurity techniques and recommendations that learn from adversarial strategy and past reform issues. DHS and cybersecurity scholars note that IT-OT monitoring is broadly effective against state-supported cyber actors because it can automatically create alerts or block suspected attacks when it detects intrusion behaviors. However, the analysis does not extend to specific adversaries like Russia.[78,79,80]

Based on current research, it is unclear if major adversaries emit detectable cyber behaviors during a cyber intrusion that allow IT-OT monitoring to intervene. This study begins to fill these gaps by focusing on Russia because of Moscow's destructive view of OCO and increasingly aggressive attacks against critical infrastructure since 1999. The subsequent analysis will compare multiple offensive Russian cyber cases to determine if they illustrate observable signatures that IT-OT monitoring could detect, and thus, mitigate. Afterward, the study will build a policy strategy based on the comparative results to increase IT-OT monitoring's adoption while addressing the strained private-public cybersecurity relations highlighted during American reforms in the 2000s.

---

[78] DHS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 15-32

[79] Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath and H. Raghav Rao. "Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear-phishing Email," in *IEEE Transactions on Professional Communication*, vol. 55, no. 4, p. 345-347, Dec. 2012, doi: 10.1109/TPC.2012.2208392.

[80] Tracey Caldwell. "Spear-Phishing: How to Spot and Mitigate the Menace." *Computer Fraud & Security* 2013, no. 1 (January 2013): p. 11–13. https://doi.org/10.1016/S1361-3723(13)70007-1.

Methodology[81]

Comparative Case Studies of Russian Cyber-Attacks

As noted by DHS, threat-informed surveillance systems – such as IT-OT monitoring – rely on programable logic that learns observable intruder behaviors to create alerts or block attacks. Thus, for modern surveillance to function, the intruder needs to exhibit abnormal behavioral patterns outside the bounds of an authorized user that indicate malicious intentions. For example, forging email addresses to mimic known accounts, using credentials to create external server connections, or stealing logins to unnecessarily access sensitive data.[82,83,84]

This study examines Russian cyber-attacks to determine if they create observable behaviors because these conditions allow IT-OT monitoring to function. The study examines the 2007 DDoS attack against Estonia's communication and financial systems, the 2015 malware attack against Ukraine's electrical grid, and the 2016 hacking of US political parties – case selection explained in greater detail below. By comparing these attacks, the study builds a set of common Russian tactics. It then identifies if these result in abnormal cyber behavioral traits – warning signs that threat-informed surveillance would detect and mitigate. The study then combines these results into a standard Russian cyber kill chain that represents Moscow's offensive approach to critical infrastructure to identify which parts of their operations are the most vulnerable to IT-OT monitoring. This study defines effective mitigation as stopping the cyber-attack, slowing the intrusion

[81] Please see appendix 2 for a deeper discussion on potential methodological counter arguments.
[82] DHS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 15-32
[83] Wang et al, 345-347
[84] Tracey Caldwell, 11–13

down, or creating alerts before breaching a sensitive system. If observable behaviors are present, IT-OT monitoring will have the capability to alert network defenders or automatically block intruders – as previously defined by DHS.

The study's comparative case analysis across the three Russian cyber-attacks represent Moscow's switch to destructive measures against critical infrastructure – a departure from 1999. Each case is similar because the operations resulted in damage to critical infrastructure as defined in this analysis; this similarity enables comparisons. However, the attacks used different offensive techniques – diverse variables – which satisfies the requirements for comparative methods. The cases will examine how Russia infiltrated and attacked the target to identify common cyber TTPs (Tactics, Techniques, and Procedures) and understand if these tactics have observable behaviors or signatures that allow IT-OT monitoring to intervene.

The study's methodology tests how the independent variable – IT-OT monitoring – affects the dependent variable – the success rate of offensive Russian cyber TTPs against critical infrastructure. The success rate is a nation's ability, specifically Russia, to use an offensive cyber TTP to expand an intrusion or levy damaging effects consistent with the earlier definition of offensive cyber operations. The results drive policy recommendations to help the adoption of threat-informed surveillance while learning from American reform efforts in the 2000s.

Case Selection Reasoning

Since the attacks against Estonia, Ukraine, and America use different tactics, the study excluded the 2008 DDoS (Distributed Denial of Service) operation against Georgia. Both the Estonian and Georgian cyber-attacks were DDoS-based, and Russia likely used

the OCO against Georgia to enhance conventional military operations immediately afterward. Timing cyber and military strikes together introduces the concept of hybrid war, which is out of scope for this study. The study's methodology focuses on defensive cybersecurity techniques and identifying observable Russian cyber warning signs.[85]

It is also necessary to address the Ukraine case. Current scholarship indicates Russia maintained a significant degree of control over the Ukrainian cyber domain by 2015, potentially suggesting a diminished comparative value of the malware induced blackout. Ukraine's reliance on Russian e-services, such as email, helped Russian cyber actors access Ukrainian communications and critical infrastructure.[86] These circumstances make OCO easier, but they do not diminish the cyber-attack's methodological value. The TTPs involved remains significant because of the time, complexity, and scope of the operation. Despite Russia's control over Ukraine's cyberspace, the 2015 attack against the electrical grid remains the first known OCO that successfully induced a large-scale electrical failure. Excluding the 2008 Georgian operation and using the Ukraine attack enables a consistent application of comparative methods. Each case represents a significant cyber operation against critical infrastructure with unique tactics.

Limitations on Sources

The cases rely on scholarly research that describes Russian cyber-attack TTPs, trade association reports, or unclassified government documents highlighting Russian cyber activity and the intrusion behavioral traits. Primary sources originated from the SANS Institute, the Department of Homeland Security, the Office of the Director of

[85] Connell and Vogler, 17-18
[86] Giles, 62-63

National Intelligence, the Department of Justice, the Swedish Defense Research Agency, Estonia's NATO Cooperative Cyber Defense Center of Excellence, the Russian Presidential Executive Office, and the Russian Ministry of Defense. These sources include studies that had access to Russian malware. Unfortunately, the author's limited computer science knowledge prevented a quantitative approach that identifies coding signatures in Russian cyber-attacks. Additionally, the author cannot speak or read Russian and did not have access to a translator. These limitations made access to Russian sources impossible unless a translation existed – translation software is unreliable with the Russian language.

Furthermore, the author only accessed technical information regarding Russian cyber-attacks available to the public – restricting the kinds of case studies and type of analysis conducted. The data restriction requires the study to use past case studies to determine if Russian TTPs create conditions that generate observable traits for effective IT-OT monitoring – current threat data remains limited. Data limitations also restricted this study's capability to examine reforms during the 2000s in other Western-aligned nations. Upon reviewing existing literature, studies with broader comparative cases across multiple countries used methodologies that relied on custom interviews of in-country personnel and special agreements to review policy documents not easily accessible by the public. Current restrictions on travel and in-person meetings make a multi-country investigation infeasible, which is why the lessons-learned focus on the US because of publicly available policy documents and a large body of scholarship.

Data: Case Studies on Russian Cyber-Attacks

2007 Operation Against Estonia: Trigger Point (April 2007)

On April 26, 2007, Estonia's Government moved a statue that honored Soviet World War Two soldiers from the central square in Tallinn, the capital, to the city outskirts. Russia protested this act and called for the resignation of Estonia's parliament. Moscow later unleashed DDoS (Distributed Denial of Service) attacks against Estonian networks to halt internet communications, financial transactions, and government services. These cyber-attacks caused extensive stoppages in critical infrastructure.[87,88] Estonia is one of the most internet-dependent countries because it relies on a national digital ID program and a country-wide data-sharing layer called X-Road to increase interoperability between businesses and government. Over 2,300 public and private services use X-Road, and nearly 100% of Estonian citizens enroll in the digital ID program to access e-services, making internet disruptions highly debilitating.[89]

Understanding a DDoS Attack

A DDoS attack relies on flooding the target with network traffic. The increased information flow disrupts legitimate server usage, preventing users from accessing the target service or system. One way to conduct this kind of attack is through a botnet, which Russia used against Estonia. Botnets are a linked web of computers infected by malware, typically between 3,000 and 10,000, controlled by a hacker to overload a target

---

[87] Roland Heickero. "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations." Defense Analysis. FOI, Swedish Defense Research Agency, March 2010. p. 39-42, http://www.highseclabs.com/data/foir2970.pdf.

[88] Michael Lesk. "The New Front Line: Estonia under Cyber Assault," in *IEEE Security & Privacy*, vol. 5, no. 4, p. 76, July-Aug. 2007, doi: 10.1109/MSP.2007.98.

[89] Kattel, Ranier, and Ines Mergel. "Estonia's Digital Transformation." In Great Policy Successes, edited by Paul 't Hart and Mallory E. Compton, First edition., p. 143–45. Oxford, United Kingdom; New York, NY: Oxford University Press, 2019.

with network traffic. The exponential amount of activity uses the victim's bandwidth capacity, causing services to stop.[90,91]

Two DDoS Waves (April 2007 – May/June 2007)

By April 28, the first wave of attacks began targeting the "Estonian Government Briefing Room, the Estonian Ministry of Defense, and leading political parties in the country."[92] The initial wave had minimal impact because it was mostly unorganized Russian hackers from Russian. However, on May 8 and 9, Russian cyber actors unleashed the second DDoS wave that hit vital parts of Estonia's critical infrastructure. Estonia's parliament, two of its largest banks, nearly every government ministry, and six of the largest news organizations were all overloaded by botnet traffic.[93,94] The attack used about 1 million computers, and the traffic volume reached 100 megabytes per second at its peak. According to the US-CERT, although the attack's scale is alarming, it is not overly complicated.[95] The rental cost for a typical botnet with 3,000 to 10,000 computers on the black market is approximately $1,000 to $5,000, making the cost of the Estonia attack roughly $500,000. Furthermore, at the time, the largest DDoS attack measured 40 gigabytes per second at its peak – one gigabyte is equal to 1,000 megabytes. For a nation with Russia's capabilities, the 2007 DDoS against Estonia is quite achievable.[96,97]

---

[90] Heickero, 39-42
[91] Lesk, 76
[92] Heickero, 40
[93] Ibid
[94] Ottis Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Tallinn, Estonia: Cooperative Cyber Defense Centre of Excellence, July 2008. p. 1-3, http://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.
[95] Heickero, 42
[96] Ibid, 41-42
[97] Lesk, 76

However, the cyber-attack's targeted nature highlights several other dangers because Russia was able to identify the necessary parts of critical infrastructure to force a full internet shut down that impacted over 60% of the country.[98,99] Since Estonia is a small nation, the DDoS network traffic overloaded its servers, forcing it to stop outside internet connections. Larger nations like the US would likely absorb an attack the size of the 2007 operation. If Russia had targeted only one sector, such as financial services, Estonia would probably not have used drastic measures. Since Moscow systematically targeted key pillars of critical infrastructure responsible for daily operations – public services, communications, and the economy – Estonia had few courses of action other than to isolate itself from the outside world.[100]

Implications of the Operation

Estonia remains highly reliant on online infrastructure to run the nation, and before the 2007 attack, the country claimed it was a "paperless government."[101] The DDoS attacks resulted in damages worth at least several millions of dollars – although the total loss is unknown.[102,103] However, the danger of the attacks was Russia's ability to disrupt several Estonian society pillars systematically. Russian cyber actors also gained access to data on several critical infrastructure sectors. The information's value was its ability to enhance future offensive cyber operations against similar critical

[98] Connell and Vogler, 13
[99] Lesk, 78
[100] Ottis, 2-6
[101] Lesk, 76
[102] Kozlowki, Andrzej. "Comparative Analysis of Cyberattacks on Estonia, Georgia, and Kyrgyzstan." In International Scientific Forum, 3:236–45. Tirana, Albania: European Scientific Institute, 2013. https://www.researchgate.net/profile/Nnedinma_Umeokafor/publication/260107032_International_Scientific_Forum_ISF_2013vol3/links/02e7e52f964505c201000000.pdf#page=246.
[103] Schmidt, Andreas. "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012." In The Estonian Cyberattacks, edited by Jason Healey. p. 1-15 Vienna, VA: Cyber Conflict Studies Association, 2013.

infrastructure.[104,105,106] The 2007 DDoS attacks resulted in a cyber blockade that isolated Estonia and was one of the first known offensive Russian cyber operations that damaged an adversary's critical infrastructure.

Key Russian OCO TTPs in Estonia and IT-OT Monitoring

Figure 2 illustrates the cyber kill chain for the DDoS attack against Estonia, and it reveals two broad tactics – target surveillance and attack vector deployment. In Estonia, most financial, government, and news services were online at the time, making it simple for an informed cyber actor to understand the crucial organizations responsible for the country's daily operations. Since several firms and government organizations managed their services through websites, the attackers used this to locate unsecured public IP (Internet Protocol) addresses to disrupt the website servers with the botnet.[107]

Figure 2: Estonia Cyber Kill Chain and IT-OT Monitoring Intervention Points

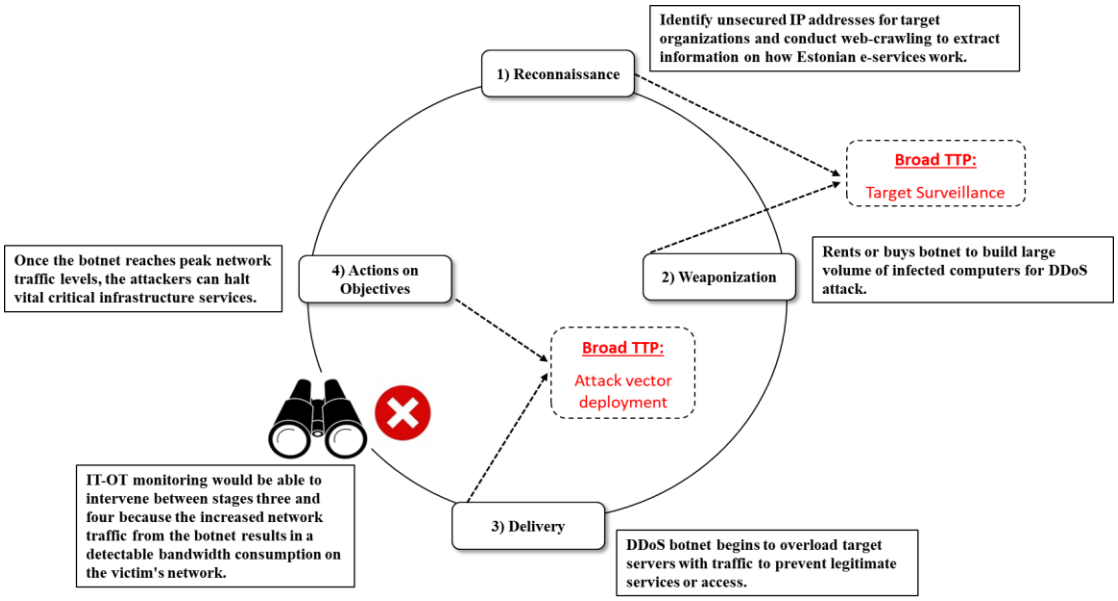


Figure 2 does not have all seven cyber kill chain stages because a DDoS attack is a less complicated offensive cyber operation than custom malware intrusions. Binoculars denote IT-OT monitoring intervention points.

[104] Lesk, 76-79
[105] Rain, 2-6
[106] Heickero, 39-43
[107] Ottis, 2-6

If the victim does not secure technical identifying information, such as an IP address, it becomes a vulnerability. A cyber actor can use the data to target website server architecture and deploy the desired attack vector. In Estonia, Russia leveraged the botnet to exponentially increase network traffic to several web servers, preventing legitimate users from using multiple vital online services.[108] When the botnet surges traffic, this action exhibits distinguishing and detectable traits during the delivery or action on objectives stage in the kill chain. The increased network activity and bandwidth drops result in measurable data consumption that surveillance systems, such as IT-OT monitoring, can detect if configured to observe external connection points. Detecting and recognizing increased traffic and extensive bandwidth usage is crucial for future mitigation.

2015 Operation Against Ukraine

Russia's offensive cyber operations against Ukraine's electrical grid remains one of the most significant cyber-attacks because it is the first known case where cyber actors shut down power for over 220,000 people.[109] Unlike the 2007 DDoS against Estonia, the 2015 operation was a concerted effort to breach internal systems and compromise critical infrastructure. The operation was likely in response to several events. These included Ukrainian legislation that would nationalize private utility firms with connections to

[108] Christos Douligeris and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." *Computer Networks* 44, no. 5 (2004). p. 650-652. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.7118&rep=rep1&type=pdf

[109] Robert M. Lee, Michael J. Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid." Defense Use Case. Washington, DC: SANS-ICS and E-ISAC, March 18, 2016. p. 1-2. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Russian oligarchs and pro-Ukrainian activist attacks on Russian controlled substations in Crimea.[110]

Understanding Spear-Phishing and Malware in Ukraine

Spear-phishing was the delivery method that Russian cyber actors used to insert malware into Ukraine's electricity providers. When an attacker uses spear-phishing, they purposely deceive the victim, usually over email, to willingly give up sensitive information – passwords are the most common target. However, the attacker can also use this vector to deliver malicious programs – malware – making email a popular distribution method.[111] In most cases, the malware hides in an attachment, and this is what occurred in Ukraine. The attackers created custom spear-phishing emails that tricked users into opening the message, allowing malware to offload itself into the network.[112,113]

The primary malware programs involved were Black Energy 3 (BE3) and Kill Disk. The BE3 malware mostly focused on harvesting credentials and establishing connections to external server points controlled by Russia. Increased access allowed the attackers to move more freely through the Ukrainian networks. Kill Disk was part of the final stages by allowing the cyber actors to erase files and damage applications used to manage operational technology like circuit breakers.[114,115]

---

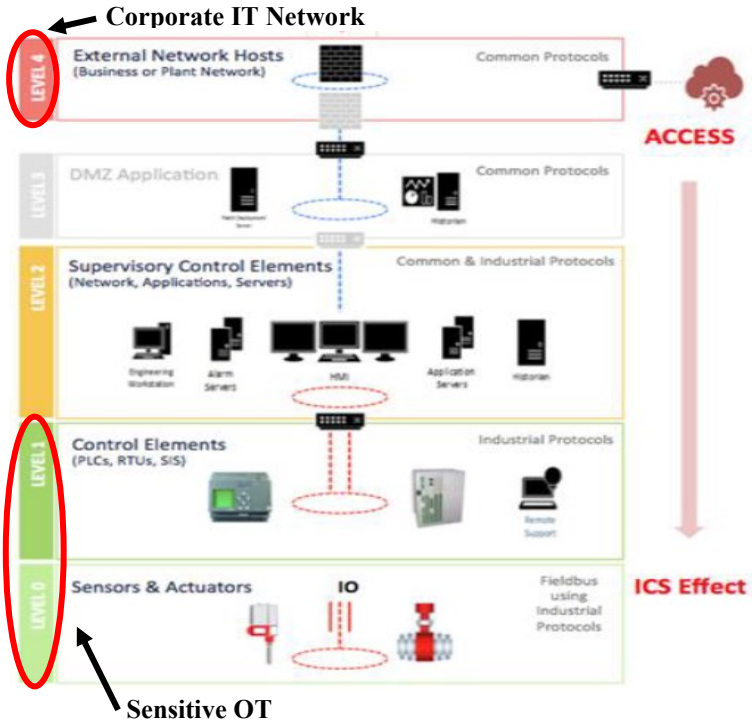
[110] Connell and Vogler, 14-23
[111] Lee et al. 5-8
[112] Ibid
[113] "Cyber-Attack Against Ukrainian Critical Infrastructure." ICS Alert 16-056-01. ICS-CERT Alerts. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, August 23, 2018. p. 1-2, https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.
[114] David. E. Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, 2017, p. 1-5, doi: 10.1109/CPRE.2017.8090056.
[115] Lee et al. 1-10

Attack Set up (July 2015 – December 2015)

Although the Ukraine cyber-attack occurred on December 23, 2015, the operation took at least six months to prepare. Russian attackers penetrated multiple Ukrainian utility firms using spear-phishing.[116] The total number of spear-phishing emails sent remains unclear, but it is likely between 50 and 100 because the subsequent malware attacks impacted at least 50 electrical substations.[117,118,119] Russian cyber actors used spear-phishing to deliver the Black Energy 3 malware to multiple utility providers and used stolen credentials for several months to probe the corporate network for weaknesses.[120,121] The cyber actors initially entered through the corporate IT network; however, as they obtained legitimate credentials, they manipulated the connections between the various network layers to move from the corporate side to sensitive OT sections – see figure 3.[122,123] These areas were the ICS (Industrial Control Systems) networks that governed HMIs (Human Machine Interfaces) – often physical workstations with specialized equipment – responsible for processes like power distribution.

[116] Ibid
[117] Ibid
[118] Lee et al. 1-8
[119] Whitehead et al. 1-5
[120] Ibid
[121] DHS, "Cyber-Attack Against Ukrainian Critical Infrastructure," 1-4
[122] Julia E. Sullivan and Dmitriy Kamensky. "How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid." The Electricity Journal 30, no. 3 (April 2017): pp. 31-33. https://doi.org/10.1016/j.tej.2017.02.006.
[123] Lee et al. 1-5

Figure 3 – Ukraine Attack Progression[124]



Attack Execution (December 2015)

The affected HMIs were part of a Supervisory Control and Data Acquisition (SCADA) environment to manage physical processes. SCADA systems often connect to a broader ICS network that leverages IT to automate OT processes like electrical power management. Once in the ICS networks, the attackers deployed the Kill Disk malware to erase files in the SCADA environment, interrupt several electrical processes, and then manipulate the circuit breakers to cause the blackout.[125,126,127] The blackout impacted three regions, including Kyiv, Prykarpattia, and Chernivtsi. The grid for these regions serves at least 3 million people. Comparatively, 220,000 people losing power is low. However, this attack's danger comes from its targeted and coordinated nature rather than

[124] Ibid, 5
[125] DHS, "Cyber-Attack Against Ukrainian Critical Infrastructure," 1-2
[126] Lee et al. 1-10
[127] Whitehead et al. 3

the size of the affected population. The cyber actors demonstrated precise knowledge of ICS-SCADA systems, and their ability to target specific substations highlights the dangerous sophistication and accuracy of this attack. Furthermore, although the blackout impacted a comparatively small number of people, the grid lost over 130 Megawatts (MW) of power in six hours – the grid's projected daily output is between 400 and 520 MW. The estimated financial loss for an attack of this scale is up to $6 billion, making the Ukraine attack costly in both money and power.[128,129,130,131]

Implications of the Ukraine Operation

Unlike the Estonia attack, where the country responded by shutting down external internet connections, Ukraine faced difficulty organizing a timely response to limit the damaging blackout. By the time Russian cyber actors were able to deploy the final malware, the Ukrainian utility firms were already severely compromised. Although Ukrainian firms and government response teams eventually expelled the Russian cyber actors and hardened existing network defenses with NATO support, Moscow already achieved its goals.[132] The 2015 cyber-attack represented a significant escalation of Russia's cyber capabilities. The Russian OCO against Ukraine demonstrated Moscow's capability to manipulate linked IT architecture to create highly destructive effects.[133]

Russia's OCO against Ukraine highlights how the interconnection from IT-OT convergence can become a critical weakness. Russian cyber actors used the layered

[128] Ibid, 1-3
[129] Lee et al. 10-20
[130] Sullivan and Kamensky, 30-35
[131] "The Cost of Malicious Cyber Activity to the U.S. Economy." Washington, DC: The Council of Economic Advisors, February 2018. p. 30-43. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.
[132] Sullivan and Kamensky, 31-32
[133] Connell and Vogler, 1-2; 19-22

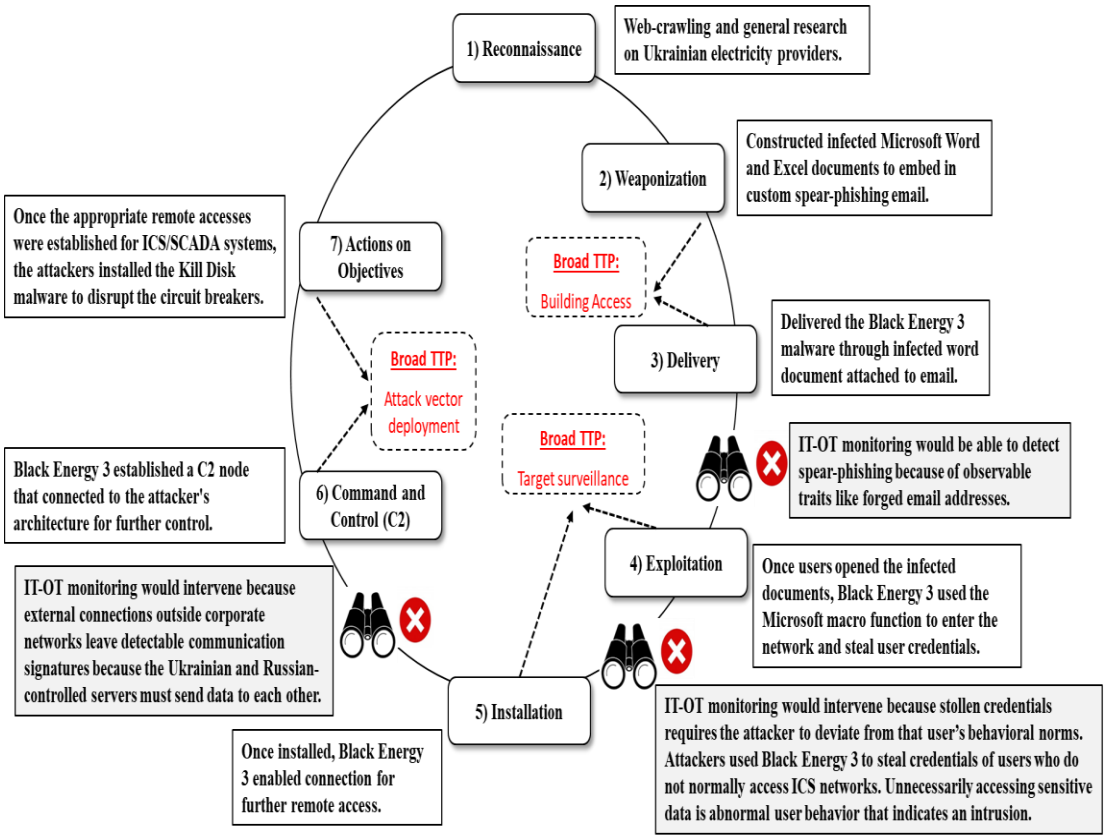
connections between the less secure Ukrainian corporate network and sensitive ICS against utility providers. By covertly acquiring access credentials and manipulating connector points, defenders had little warning of the attack. These lessons underscore the need for IT-OT monitoring that surveils all networks for abnormal cyber behavior.

Key Russian OCO TTPs in Ukraine and IT-OT Monitoring

The Russian cyber-attack against Ukraine's electrical grid highlights several critical TTPs. The attack relies on first building accesses. In Ukraine, this happened through email-based spear-phishing that delivered the initial malware payload, BE3. The next TTP was network surveillance. Although this tactic has similarities with Russia's attack against Estonia in 2007, the cyber actors conducted internal surveillance through stolen access credentials in Ukraine. In 2007, cyber actors conducted external network surveillance to identify unsecured public information. The use of legitimate credentials enabled Russia to find connection points into the ICS network and deploy their attack vector – the final major TTP. The attackers deployed the Kill Disk malware into several operational technology processes to disrupt services and enable the blackout's conditions.

The 2015 offensive cyber operation against Ukraine's electrical grid reveals a sophisticated and well-planned methodology focused on clandestine accesses. However, like Estonia, Russia's tactics create observable traits that systems, such as IT-OT monitoring, can detect. Figure 3 aggregates the Ukraine operation data to present a cyber kill chain that also displays IT-OT monitoring intervention points.

Figure 3: Ukraine Cyber Kill Chain and IT-OT Monitoring Intervention Points



The initial access building through spear-phishing and subsequent surveillance using stolen credentials are the most likely points where surveillance systems can detect an intrusion. Spear-phishing is a popular tactic with other state-supported cyber actors and criminal groups, making behavioral markers, such as forged emails, odd grammar, or hidden links, well-known and measurable by threat-informed surveillance.[134]

Likewise, unauthorized users using stolen credentials will likely deviate from an authorized user's behavioral patterns to connect with other networks. In Ukraine, BE3 allowed the attackers to steal users' credentials that would not usually have access to the ICS networks and establish an external server connection. These deviate well outside

[134] Caldwell, 11–13

average user norms because it requires accessing sensitive information constrained to a select group and creating a connection that links to servers outside the corporate network. When two servers communicate, they need to send data to each other, and this is where surveillance can detect external communication. A properly-configured IT-OT monitoring system would detect these behaviors because of the unnecessary attempts to access sensitive data and external connection points. Unfortunately, monitoring technology is unlikely to stop the attack if a cyber actor enters the ICS network. Therefore, it is crucial for surveillance systems to examine all entry points – internal and external – to create a more alert point. Detecting spear-phishing or the misuse of credentials over IT and OT networks is essential for preventing future Russian OCO.

2016 Hacking and Dumping Operation Against the US

In contrast to Russia's 2007 and 2015 cyber-attacks, the 2016 hack and dump operation did not have a particular triggering event. The Office of the Director of National Intelligence (ODNI) indicates that the cause was likely a combination of events. These include Russia's preference for President Trump, a longstanding view that the US-led liberal world order is a threat to the Putin regime, and even the Olympic doping scandal.[135] The ODNI claims that the Russian hack and dump operation was part of a broader effort to influence the 2016 elections, including Russian propaganda and online information operations – though there is no evidence of tampering with voting architecture.[136]

The study focuses on the hack and dump operation because it used intentional destructive methods to compromise private networks, which aligns with the earlier

[135] ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," 1-2
[136] Ibid, iii, 2-3

definition of Offensive Cyber Operation. However, the study acknowledges the significance of concurrent online information operations that benefited from these hacks.[137] Although Russia's hacking operations did not result in visible damage, the hack and dump activities directly attacked the US political process.[138] The operation's intentions and tactics highlight Moscow's desire to disrupt American processes vital to the nation's successful operation.

Attack Set-Up (March 2016)

According to the US Department of Justice, Russian cyber units associated with the Main Intelligence Directorate of the General Staff (GRU) purposely breached email accounts in the Clinton Campaign, Democratic Congressional Campaign Committee (DCCC), and the Democratic National Committee (DNC) to steal confidential documents.[139] The cyber actors implanted several kinds of malware that allowed them to exfiltrate the data. Russia leaked the stolen documents to the public using online personas and the WikiLeaks organization – hence the term hack and dump.[140] Russian cyber actors started the operation months before the onset of the 2016 US Presidential election. By March 2016, Russia dispatched 90 spear-phishing emails to various levels of the Clinton campaign. The targets ranged from junior staffers to the campaign's chairperson, John Podesta.[141] Both official emails with at hillaryclinton.com addresses and google accounts

[137] Ibid, 3-5
[138] ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," 2-3
[139] Robert S. Mueller III. "Report on The Investigation into Russian Interference in the 2016 Presidential Election." Attorney Work Product. Washington, DC: US Department of Justice, March 2019. p. 36, https://www.justice.gov/storage/report.pdf.
[140] Ibid, 37-38
[141] Ibid, 37

were subject to the operation's spear-phishing, which allowed Russian cyber actors to access multiple accounts at numerous levels – including John Podesta.[142]

Understanding the Types of Malware

Unlike Estonia and Ukraine, the 2016 US hacking operations saw a significant increase in malware volume. The Ukraine case highlighted two major malware programs, while the US exhibited four. Furthermore, unlike the Kill Disk program, which required manual control by the attacker, the malware used against the US was mostly automated. Like BE3, Mimikatz aided credential theft. Attackers then installed X-Agent to secure control over the victim, as it logs keystrokes and takes screenshots. X-Tunnel enabled a secure connection between the victim and external GRU-controlled computers. Finally, Rar.exe compressed documents for mass exfiltration. These malware programs represent increased sophistication and improved efficiency over the Ukraine operation only one year before.[143,144,145]

Access Propagation and Data Exfiltration (April 2016)

By April 2016, Russia gained access to the Clinton campaign and DCCC through its spear-phishing. Russia also used a DNC employee's Virtual Private Network (VPN) connection to access their mail servers.[146] A VPN enables individuals to access a private network remotely through existing internet connections. It is not clear how Russia gained access to the VPN, but it was likely unsecured, or the user had poor security hygiene – weak passwords, for example. Attackers then used Mimikatz, X-Agent, X-Tunnel, and

[142] Ibid
[143] Mueller, 38-39
[144] Whitehead et al. 2-3
[145] ODNI, "Assessing Russian Activities and Intentions in Recent US Elections," 1-5
[146] Ibid, 37-38

Rar.exe to enable data exfiltration. The cyber actors stole over 300 gigabytes of election-related data.[147]

Public Exposure (April 2016 – November 2016)

Between late April and June, the GRU publicly posted thousands of documents through two online personas, DCLeaks and Guccifer 2.0. By July, the Guccifer persona transferred document archives to the infamous disclosure group, WikiLeaks.[148] On July 22, 2016, three days before the Democratic National Convention, "WikiLeaks released over 20,000 emails and other documents stolen from the DNC computer networks."[149] These leaks continued until the day before the 2016 election. Between October and November, WikiLeaks leaked more than 50,000 documents from John Podesta's email – including private speeches made by Hillary Clinton.[150] According to Federal Election Commission campaign finance data, between 2016 and 2017, the DNC spent over $500,000 on technology services with Crowdstrike – a cybersecurity firm known for exposing Russian cyber efforts in 2016. The payments began in May 2016, shortly after GRU cyber actors exfiltrated data in April. The timeline suggests the payments were for mitigation efforts surrounding the Russian hacks; however, this does not include other organizations involved in remediation, such as law firms. The attack's total cost for the DNC likely reaches over $1 million.[151,152]

---

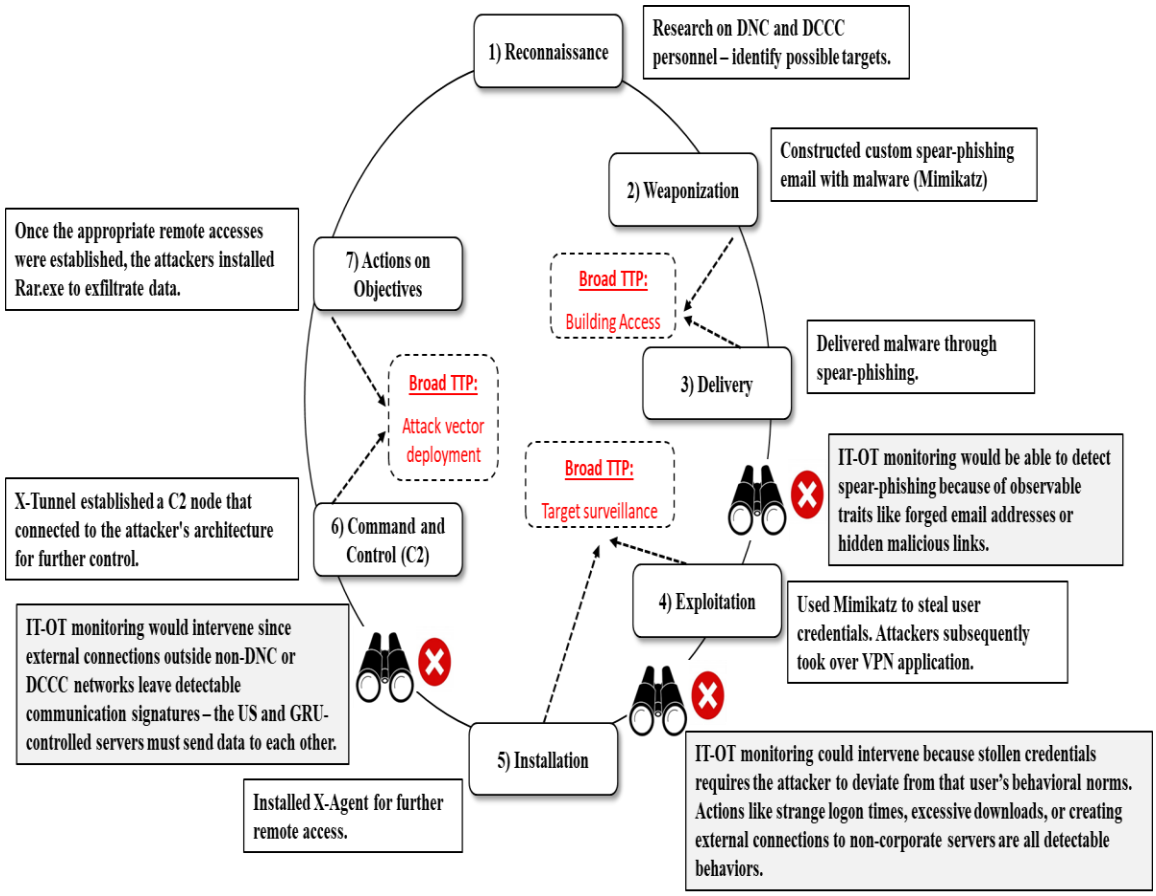
[147] Mueller, 39-50
[148] Ibid, 40-46
[149] Ibid, 46
[150] Ibid, 48
[151] FEC.gov. "Campaign Finance Disbursements: Crowdstrike." Federal Election Commission. https://www.fec.gov/data/disbursements/.
[152] "Our Work with the DNC: Setting the Record Straight," June 5, 2020. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Russia's intentions were harmful and purposely designed to disturb the core political process fundamental to any republic, the democratic election of a new leader. The hack and dump OCO against the Democratic Party used destructive technical means to breach private networks, steal thousands of documents, and then leak the material. These acts almost certainly focused on tainting US political institution legitimacy, making it one of the most significant Russian cyber-attacks.

Key Russian OCO TTPs in the US and IT-OT Monitoring

The 2016 Russian hack and dump operation against the US reveals TTPs that have some similarities with the 2015 cyber-attack against Ukraine – though there are differences in the tactics' execution. Like the Ukraine case, Russia started by building accesses through spear-phishing. This popular tactic remains effective because even with good user awareness or phishing detection systems, it is challenging to eliminate human error. The next major TTP is network surveillance, which also occurred in Ukraine. However, in the US, this step complimented the attack vector deployment. Unlike the Ukraine attack, the cyber actors had to traverse fewer security layers in 2016 because they were not breaking into sensitive ICS networks. Furthermore, because the hack and dump intrusions focused on stealing data, the malware involved did not create destructive effects. Instead, the programs mostly focused on locating and exfiltrating the victim's information. In contrast to past operations, Russia focused on public exposure to achieve its end-state in the US, and this TTP is not exclusively cyber-based. Russia used online platforms and personas to disseminate private information, but this is not reliant on a specific cyber technique.

Figure 4: US Cyber Kill Chain and IT-OT Monitoring Intervention Points



Although Russia's destructive phase differs from previous cyber-attacks, preventative lessons remain consistent with other operations. Situational awareness and early detection are the primary mitigation takeaways in the US case because stopping cyber actors when they try to establish accesses or conduct extensive surveillance can halt the operation. Figure 4 illustrates the US attack's cyber kill chain and the intervention points for IT-OT monitoring. Like Russia's Ukraine operation, IT-OT monitoring systems have a high probability of intervention and mitigation if they focus on detecting spear-phishing attempts, the misuse of credentials, or external connections. Spear-phishing has several observable traits already discussed, and compromised users obtained sensitive data – such as private speeches – they would not typically be able to access.

Furthermore, attackers also created several external connections to non-DNC or DCCC servers through X-Agent and X-Tunnel, creating a detectable communication signature because of data exchange between US and GRU-controlled servers. These tactics have measurable traits that present opportunities for defenders to discover before an attacker can exfiltrate the target data or deploy malware – stages where surveillance would do little to prevent further damage. While the 2016 hack and dump operation against the US Democratic Party is a unique OCO targeting non-traditional critical infrastructure, it still highlights vital lessons for defenders.

Discussion: Comparing Case Study Data

Common Russian Offensive Cyber TTPs

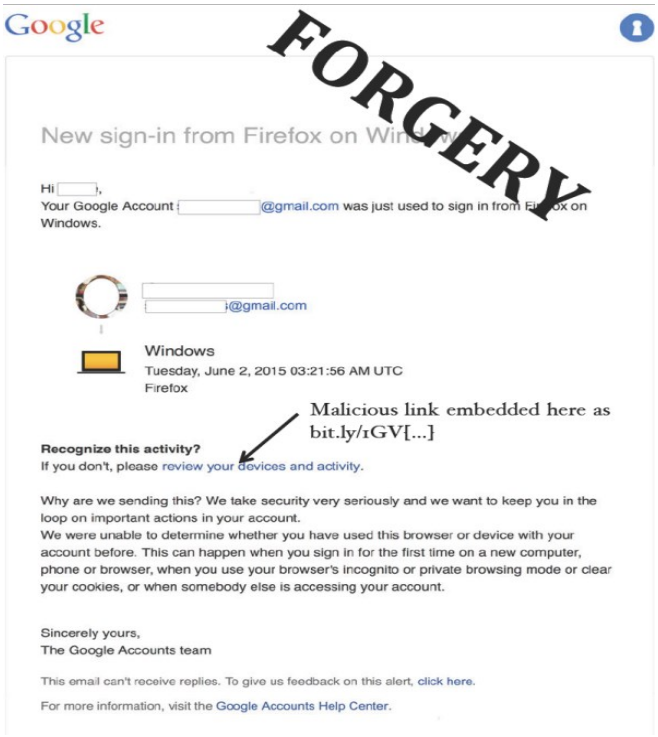
Table 3 combines the study's findings across each case and illustrates several trends. Three common TTPs appear, include building accesses, target surveillance, and attack vector deployment. However, the data revealed that each TTP used unique methods of accomplishment specific to the operation. When analyzing each of the tactics, it is critical to consider the various methods used in their corresponding cases.

Common Russian Offensive Cyber Behavioral Traits

Most importantly, Table 3 illustrates that Russia's tactics did create observable behavioral traits that IT-OT monitoring could detect in over half of the tactics. Broadly, these focused on three behaviors – analyzed in greater detail below. First, building access through spear-phishing was one of the most common TTPs. Spear-phishing often requires fake addresses to mimic known emails, like a Gmail password reset, to trick users. Most threat-informed surveillance systems can detect because they contain databases of known

email types. Additionally, spear-phishing often uses malicious links embedded in the email, and these web addresses are observable – see figure 5.

Figure 5: Example Russian Spear-Phishing Email[153]



Second, Russian cyber actors favored conducting target surveillance through stolen credentials. These tactics require deviating outside the victim's regular operating routines. In several cases, the login information led to unnecessarily accessing sensitive information and creating external connections to unsecured servers – all apparent behavioral traits that indicate an intruder. Finally, when Russian attackers deployed a DDoS (Distributed Denial of Service) attack, the volume-based attack leaves a significant data signature because of increased data consumption as bandwidth drops. According to DHS, Knapp, and Langill, IT-OT monitoring would detect these behaviors because the

[153] Rid, Thomas. Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Pub. L. No. 033017, § US Senate Select Committee on Intelligence, 1 (2017). p. 7. https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf.

systems use a library of open source and private data to create cyber-attack profiles, enabling the automatic detection when activity deviates outside user norms.[154,155,156]

Table 3 also highlights a critical caveat. Although Russian OCO tactics created observable behaviors in over half of the cases, almost all correspond to set-up phases, indicating that IT-OT monitoring is mostly a preventative measure. Unfortunately, if an attacker can set up their attack, threat-informed surveillance would do little to stop the operation. Even if an attack vector, like malware, produced signatures, IT-OT monitoring would not stop the cyber-attack because the intruder already breached the target system. While the case studies reveal that Russian TTPs create several abnormal behavioral traits during an attack's initial phases, defenders still need to secure sensitive systems with active defenses.

Case Findings: Attack Vector Deployment Through DDoS (Estonia, 2007)

The DDoS attack vector was the only TTP used in the latter half of a Russian offensive cyber operation where IT-OT monitoring could be an effective mitigation tool. In Estonia's case, many organizations observed large increases in bandwidth consumption, likely from the external botnet connections. The increased data consumption is a measurable trait that a monitoring system could detect to alert network defenders of a possible imminent attack, giving the victim vital time to isolate web servers or shut down connections in an emergency. IT-OT monitoring can surveil external connection points and look for signs of volume-based attacks, such as large bandwidth consumption, to prevent a DDoS.

---

[154] Knapp and Langill, 30-36; 50-53.
[155] DHS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 27
[156] Ibid, 28-30

Table 2: Combined Russian OCO TTPs Against Critical Infrastructure

Russian TTP	Method of Accomplishment	Case Observed	Target Type	Results	Abnormal Cyber Behavioral Trait	IT-OT Monitoring Effectiveness	Explanation
Target surveillance	Leverage unprotected network information (e.g. IP addresses)	Estonia (2007)	Banking, government services, public communications	Located unsecured web servers for follow-on attack	No; analysis indicates this happens through anonymous web-crawling	Not effective	It is unlikely that a holistic monitoring system would be able to detect this activity, as an attacker can accomplish this discretely because the target information already had weak protections
Attack vector deployment	DDoS through botnet	Estonia (2007)	Banking, government services, public communications	Denied services for key critical infrastructure and forced Estonia to shut down external internet connections	Yes; DDoS attacks result in large data usage on the target network because of bandwidth consumption	Effective	A DDoS attack generates a large amount of network activity, and detecting the unusually high amounts of traffic on an IT network can alert network defenders to shut down external connections before the attack cripples the target
Building accesses	Spear-phishing	Ukraine (2015)	Utility provider	Gained access to multiple corporate networks for Ukrainian utility firms	Yes; spear-phishing has several known traits, such as forged email addresses or odd phrasings in the message, that are detectable by surveillance	Effective	Spear-phishing is a widely used method that can be detected by individual reporting or holistic monitoring - similar to a spam filter - and stopping the attacker at this stage would prevent the intrusion
Target surveillance	Stollen access credentials	Ukraine (2015)	Utility provider	Found connection points between IT network layers to enter sensitive ICS	Yes; using stollen credentials can result in operating outside that user's norms - e.g. accessing sensitive networks not usually needed by that user	Effective	IT-OT monitoring would be effective because the attackers would use the stollen credentials outside of that user's normal routine, unessarily accessing sensitve data for example, and this would generate alerts that cause network defenders to investigate
Target surveillance	External connection for remote control to set up C2 node	Ukraine (2015)	Utility provider	Created outside connection points to establish further control over user	Yes; most users do not create unmonitored or unsecure channels to non-coporate servers	Effective	IT-OT monitoring would be effective because the external connections must contact a non-corporate server, creating a communication signature that is dectable
Attack vector deployment	Kill disk malware	Ukraine (2015)	Utility provider	Allowed cyber actors to disrupt several critical OT processes and set up the conditions needed to cause a blackout	Partially; malware would produce several destructive results, but at this stage intervention is too late	Not effective	Although this tactic does create dectectable traits, if a cyber actor reaches this point in the operation, a surveillance system would have little impact on mitigation because the attack is already in its final stage and the damage is done
Building accesses	Spear-phishing	US (2016)	Political party/supporting organization	Gained access to multiple political IT networks	Yes; spear-phishing has several known traits, such as forged email addresses or odd phrasings in the message, that are detectable by surveillance	Effective	Like the Ukraine case, spear-phishing has several known traits, and these are detectable by either a holistic monitoring system or individual reporting
Target surveillance	External connection for remote control to set up C2 node	US (2016)	Political party/supporting organization	Created outside connection points to establish further control over user	Yes; most users do not create unmonitored or unsecure channels to non-coporate servers	Effective	IT-OT monitoring would be effective because the external connections must contact a non-DNC or DCCC server, creating a communication signature that is dectable
Target surveillance & attack vector deployment	Stollen access credentials, VPN connection, malware supporting document location and exfiltration	US (2016)	Political party/supporting organization	Stole thousands of sensitive political documents	Partially; stollen credentials can cause the cyber actor to operate outside user's defined norms, but the data exfiltration was highly encrypted and masked its signatures	Partially effective	If the surveillance system detects the misuse of credentials, it is possible to alert defenders and intervene; however, once a user's loses control of their VPN or malware enters the network, surveillance will not mitigate the operation
Public exposure	Russian-controlled online platforms and personas	US (2016)	Political party/supporting organization	Leaked thousands of confidential Clinton campaign and Democratic Party documents	No; the exposure happened outside the target and surveillance would not be able to preemptively detect this	Not effective	If a cyber actor can exfiltrate data outside the victim's network, surveillance will not be able to mitigate forms of unauthorized public disclosures

Case Findings: Building Accesses with Spear-phishing (Ukraine, 2015; US, 2016)

IT-OT monitoring systems would be effective against attackers trying to build access points through spear-phishing, as seen in Ukraine and America. Warnings like spelling mistakes or a forged email address designed to mimic a known account are learnable behaviors that modern defense systems can identify – though user education is still essential because technology can make mistakes. Additionally, when spear-phishing attempts do not have all the identifying attributes, mitigation systems can still isolate these incidents for further review by network defenders to prevent potential damage.[157,158]

Even if spear-phishing is successful, IT-OT monitoring can detect and stop an intrusion after the initial penetration because it uses multi-layered surveillance. Many holistic surveillance systems encompass several access points that could alert network defenders before the attacker reaches sensitive components – especially if the cyber actor exhibits abnormal behaviors, such as excessive attempts to access restricted areas.[159,160] Though early detection remains critical because the longer an intruder remains on the network, they will be more likely to avoid defensive monitoring.

Case Findings: Surveillance with Stolen Credentials (Ukraine, 2015; US, 2016)

A common tactic in Ukraine and American cases were stealing real login information. However, the use of these credentials' centers around a user's behavioral norms. When a user acquires sensitive information, and their position does not require the restricted data, this is a potential intrusion warning sign. Unnecessary accesses occurred

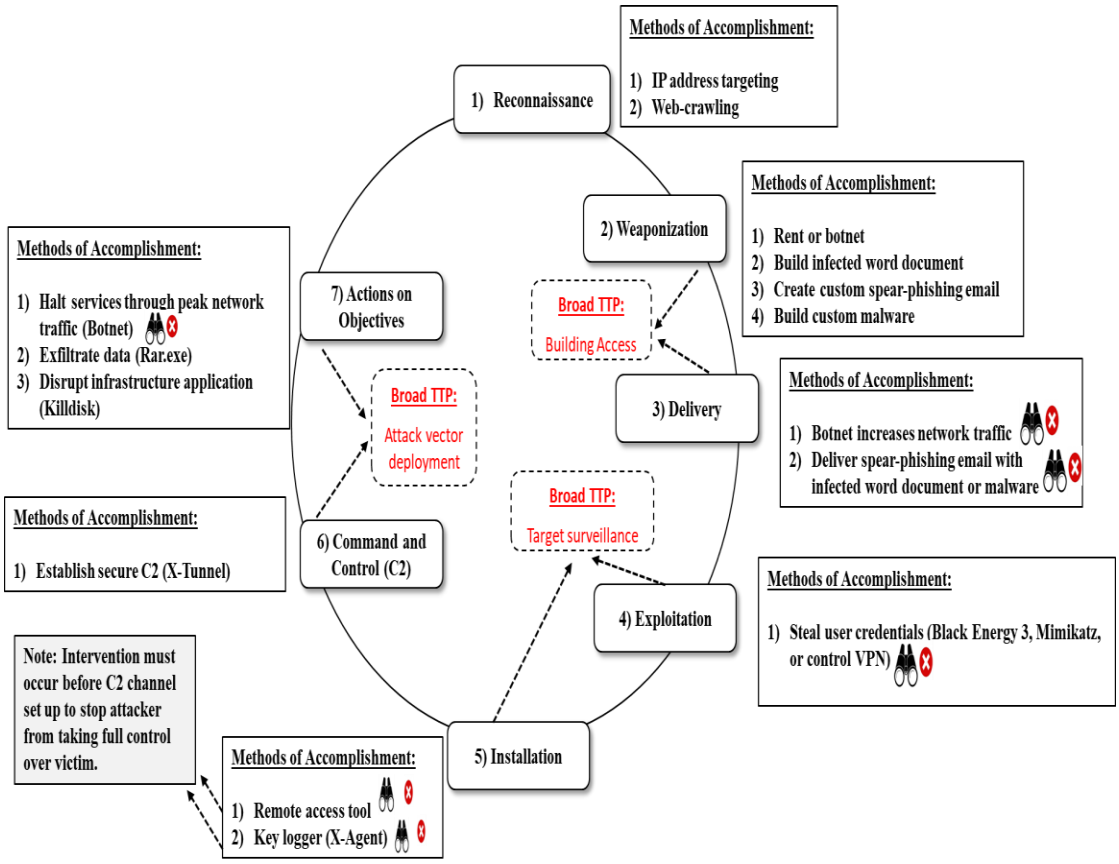
[157] Wang et al. p. 345-347
[158] Caldwell, 11-13
[159] Knapp and Langill, 30-36; 50-53.
[160] DHS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 28-30

in Ukraine and the US, and this abnormal behavior is a trait IT-OT monitoring can identify because it highlights malicious intent. Furthermore, Russia used these credentials in Ukraine and America to set up external connections for a C2 channel to control the attacker. The external connection creates an observable signature IT-OT monitoring could detect because of data exchanged between the victim and attackers' servers.

Overall Results from Comparative Analysis

The results of the comparative analysis indicate several crucial lessons. Broadly, a Russian OCO's (Offensive Cyber Operation) anatomy against critical infrastructure contains three phases – building accesses, target surveillance, and attack vector deployment. These TTPs result in several observable behavioral traits that IT-OT monitoring can detect, enabling surveillance to mitigate the attack if it intervenes during the delivery, exploitation, installation stages. The results highlight that Russian OCO against critical infrastructure is most vulnerable when the cyber actors set up the operation because they exhibit the abnormal behavior that telegraphs malicious intent – actions that deviate outside what authorized users would conduct. Unfortunately, because of the diverse tactics and tools available to Russian cyber actors, there is no standard IT-OT monitoring version that applies to all critical infrastructure. Organizations will require relevant intelligence to configure threat-informed surveillance based on the risks they face in their industries. Figure 5 summarizes Moscow's tools, techniques, and procedures over the three case studies into a standard Russian cyber kill chain for OCO against critical infrastructure while highlighting where IT-OT monitoring can intervene.

Figure 6: Russian Cyber Kill Chain



Implications of Findings in the Context of America's Reforms During the 2000s

These results indicate cyber warning signs that modern threat-informed surveillance could detect; however, the results point to a broader policy issue. Countries like the US were tracking the Russian cyber threat since at least 1999, and the 2000s demonstrated an effort to combat this problem. Unfortunately, these efforts – combined with IT-OT convergence trends – created an environment where private sector infrastructure providers do not prioritize working with the government because they perceive the coordination costs as undesirable. The broader policy question is understanding how to create policies that support the broad adoption of IT-OT monitoring while learning from past problems to incentivize better private-public

cooperation. Building a better relationship between the public and private sectors is crucial to improving cybersecurity against nations like Russia.

Policy Recommendation: Improving Private and Public Sectors Relationships

A vital lesson from analyzing Russian tactics, and the problems observed in the US's efforts to reform cybersecurity during the 2000s, is simplified coordination. A strained private-public cybersecurity relationship benefits Moscow by giving them more opportunities for infiltration. The US reforms highlighted disjointed cybersecurity and regulatory processes that contribute to decreased private sector coordination. Streamlined government authorities are the first step to improving private-public relations. Currently, DHS works with several regulatory agencies, such as the DOE and FERC, and a complex coordinating council system from the NIPP. The US approach requires private industry to work with different agencies while separating cybersecurity and regulatory authorities in the government. If DHS, or organizations like it, had the authority to conduct regulation enforcement, it would grant cyber response teams more access to private critical infrastructure providers without the pretext of a breach. These authorities are mostly under regulatory agencies' that focus on standards enforcement.

DHS could then proactively help infrastructure organizations to build defenses that are compliant with current standards before cyber-attacks occur. Most importantly, by centralizing regulation and cybersecurity authorities within the homeland security apparatus, private-public collaboration would be more straightforward. This approach empowers private industry to increase communication with cyber defense agencies because there is a central agency responsible for cybersecurity.[161] Streamlining the

[161] Parfomak et al. 4-9, 18-19

government structure is crucial because it is one of the main problems contributing to a contentious culture between private and public organizations. Although this suggestion comes from US lessons, other nations with similar government cybersecurity policies could use it.

Comparative analysis between Estonia, Ukraine, and the US revealed that Russian TTPs have several distinct signatures and abnormal behaviors that can alert IT-OT monitoring systems of a possible intrusion. The critical lesson is ensuring that infrastructure providers have current intelligence telling them the warning signs and can easily communicate with government agencies when a breach happens. Governments could adopt a program like Israel's Cyber Net, an online platform where private industry can share breach data with cybersecurity agencies and other firms anonymously. The anonymity allows firms to share data without fear of public exposure, a concern that previously stopped private organizations from disclosing breaches. The communication channel also allows governments to share intelligence quickly, giving firms critical information on adversarial warning signs for threat-informed surveillance.[162] Furthermore, because other companies can access the data, it would pressure firms that do not prioritize network defense to realign IT priorities after seeing the damage caused by breaches. Information sharing programs help change the private-sector culture, improve coordination with the government, and ensure that infrastructure providers have the most accurate intelligence to feed IT-OT monitoring systems.

[162] Marc Barrachin, and Algirde Pipikaite. "We Need a Global Standard for Reporting Cyber Attacks." *Harvard Business Review, vol.* 592, no. 6 (November 6, 2019). pg. 1–5, https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks

The comparative analysis revealed that Russian cyber actors could manipulate converging IT and OT systems because of the interconnection between networks to deliver an attack. The IT-OT convergence trend was also a factor contributing to cultural tensions between private and public organizations during American reform efforts in the 2000s, demonstrating the need to broaden access to defensive techniques, like IT-OT monitoring, which can surveil all types of systems. Government financial aid can help the private sector lower cybersecurity costs to prevent attackers from taking advantage of IT-OT connectivity. Grant programs and tax credits could help critical infrastructure providers afford commercial cybersecurity services to raise the industry's overall defensive capabilities, giving firms the tools to defend themselves. Focusing on giving companies resources also improves the private-public cybersecurity relationship by supporting industry rather than creating more government bureaucracy.

While commercial cybersecurity firms, such as McAfee, have IT-OT monitoring capabilities, they require significant customization for critical infrastructure. The requirements of a bank are different from a utility firm. Infrastructure providers that purchase these services may also need to coordinate with government agencies to ensure that the system meets regulatory standards. Purchasing commercial solutions is different from a complete IT-OT monitoring system. Supportive funding aimed at giving firms the resources to build strong cybersecurity will help proliferate threat-informed surveillance that can decrease the number of vulnerabilities caused by IT-OT convergence.[163]

Although Russian cyber-attacks have several warning signs that IT-OT monitoring can detect, a stronger private-public collaboration culture is necessary to

[163] DHS, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 5-30

ensure threat-informed surveillance is broadly adopted. The American reform efforts in the 2000s show a convoluted government-led approach to defending critical infrastructure. These experiences, and new technology trends, did not foster a strong cybersecurity culture in private infrastructure providers. Therefore, the government should build collaborative policies that support private organizations rather than creating mandates or overbearing government agencies. A cooperative balance between public and private organizations is vital for creating a culture that values stopping state-sponsored cyber-attacks. Defensive techniques like IT-OT monitoring can be effective against Russian cyber-attacks. Policymakers need to build flexible policies that support private industry and increase threat-informed surveillance's broad adoption. By focusing on providing streamlined processes, information sharing, and funding, threat-informed surveillance can be more efficient by operating in a collaborative private-public culture.

Conclusion: A Partial Solution to the Russian Cyber Threat

Russia's offensive cyber capabilities against critical infrastructure evolved significantly since 1999. Russian OCO tactics broadly focus on building accesses through spear-phishing, conducting target surveillance with stolen credentials, and using several types of custom malware, or a DDoS, to deploy their attack vectors. In over half of the observed tactics, these created observable abnormal behavioral traits that an IT-OT monitoring system can detect. The detectable characteristics highlight that threat informed surveillance would likely be an effective measure to mitigate Russian offensive cyber. However, the results highlighted that the technique could only stop the intrusion or alert network defenders during set up phases. This outcome was critical because the comparative analysis revealed that IT-OT monitoring is mostly a preventative measure.

Threat-informed surveillance cannot replace active defenses, such as extra firewalls or network vulnerability inspections. Passive surveillance systems should be part of a broader defensive solution against the Russian cyber threat.

These results supported recommendations that would help broaden the adoption of IT-OT monitoring by addressing broader policy issues identified during attempted US reforms in the 2000s. Russian strategy highlights that it thrives in a scenario where adversary disorganization creates uneven cybersecurity capabilities. It gives Moscow the capability to control the information space and levy destructive offensive cyber to degrade the enemy. Unfortunately, the problems in the 2000s supported Russia's approach. The reforms and converging IT and OT systems created a private sector culture that valued cost reduction and efficiency. Automation in IT and OT amplified a strained private-public relationship with the government because firms needed to coordinate with several agencies.

The policy recommendations call for governments to streamline their regulatory and cybersecurity agencies. Homeland security organizations, such as DHS, need regulatory authorities to decrease critical infrastructure providers' coordination costs. The suggested reforms also support more intelligence sharing processes because it gives industry the necessary information to identify Russian behavioral markers. Finally, monetary support to purchase commercial solutions would help spread IT-OT monitoring and prevent Russian cyber actors from manipulating networked architecture.

As policymakers face more aggressive and destructive Russian cyber capabilities, it is vital to create methods that combat Moscow's offensive cyber approach. Focusing on creating a collaborative private-public relationship is one of the first steps. Instead of

forcing a government-driven solution, giving industries the necessary tools while streamlining private-public coordination points is a more productive pathway.

Suggestions for Future Work

Understanding how to defend critical infrastructure from offensive Russian cyber operations is a complex topic. The study shows that although Russia telegraphs several observable abnormal cyber behaviors, the private-sector is reticent to adopt IT-OT monitoring. The policy recommendations provide suggestions for governments on how to fix cultural problems impeding threat-informed surveillance's standardization. However, investigation beyond this study would improve scholarship by understanding the specific reasons firms resist modernization.

While lessons from the 2000s suggest possible reasons for low adoption rates of modern threat-informed surveillance, more detailed analysis is necessary. Identifying the cybersecurity systems currently in use and the costs to upgrade these with threat-informed surveillance capabilities would quantify potential roadblocks. Additionally, investigating how government cybersecurity policies increase corporate costs would help tailor future policy efforts.

Finally, conducting this study for each significant adversary – China, Iran, and North Korea – would enable policymakers to have a comprehensive understanding of the entire threat landscape by identifying specific warning signs for each country's OCO. If all adversaries exhibit detectable cyber traits that IT-OT monitoring could measure, this will ensure the technique's broad effectiveness – although negative or neutral results would be equally revealing.

Appendix One: Continuous Diagnostic Mitigation (CDM) Program

The CDM program is one of the primary US federal cybersecurity programs run by CISA and works across all civilian agencies. First developed in 2012 under DHS, CISA took over CDM in 2018 after the agency's formation. However, unlike EINSTEIN 3 Accelerated, which extends to the private-sector, CDM only protects government networks.[164] The program uses custom dashboards to receive and aggregate data from several government entities using a contracting solution to distribute sensors to federal, state, and local civilian agencies. Data fusion from all government levels enables CISA to conduct asset, identity, network security, and data protection management on a large scale.[165]

Most importantly, this is another example of IT-OT monitoring because the program can monitor and fuse information from multiple networks. CDM gives CISA the capability to provide defense services across the .gov domain, and its cloud architecture enables easy technological integration.[166] The program remains a staple of US government defenses and highlights American policymakers' intent to integrate threat-informed surveillance.

[164] CDM Program Overview." Washington, DC: Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_CDM%20Program%20Overview_Fact%20Sheet_0.pdf.
[165] Ibid
[166] Ibid

Appendix Two: Responding to Counter Arguments in the Context of the Study's Methodological Approach

The study's methodology focuses on understanding past Russian cyber behavior trends to see if they create the conditions necessary for successful IT-OT monitoring. Understandably, the reliance on older data runs the risk of building an outdated study; however, this is unavoidable given restrictions in this field face. Prominent scholars who study Russian cyber capabilities such as Connell, Vogler, and Giles use similar methodology. Connell and Vogler use past Russian cyber behavior as the foundation of trend analysis for specific defensive recommendations.[167,168] Avoiding this methodological problem would require access to current cyber threat data, usually not publicly accessible until after an attack.

Furthermore, this study goes beyond understanding an established defensive technique, IT-OT monitoring, to claim that it would stop Russian cyber-attacks. The goal is to conduct foundational analysis to see if Russian offensive cyber tactics telegraph specific warning signs that IT-OT monitoring would detect given Moscow's specific destructive approach to offensive cyber. The current scholarship does show that IT-OT monitoring is broadly effective – this is why DHS recommends systems with threat-informed surveillance capabilities. However, the literature does not extend to adversary-specific analysis – a gap this study aims to fill. Current research on threat-informed surveillance is mostly at the system-level by analyzing specific types of technologies' weaknesses. With increasing aggressive Russian attacks on critical infrastructure, it is crucial to validate if IT-OT monitoring has the same degree of effectiveness claimed at

[167] Connell and Vogler, 13-28
[168] Giles, 54-64

the aggregate level. Unfavorable results can appear even if a study claims average positive results and each adversary is unique. The second defining component of this study is to provide policy recommendations on implementing IT-OT monitoring, given the lessons of US reform failures in the 2000s. These recommendations, combined with adversary-specific analysis, make the study unique among current scholarship.

Although testing baseline effectiveness is a less glamorous endeavor, it is crucial before more policy-specific research can occur. For example, a natural next-step for future research would be to understand why infrastructure providers do not use IT-OT monitoring more widely to defend against Russian cyber-attacks. However, studying reasons behind adoption rates, or lack thereof, rests on understanding threat-informed surveillance's effectiveness. If Russian tactics do not display detectable behavioral traits, then IT-OT monitoring would be ineffective against Russian offensive cyber and exploring the adoption rate would be meaningless. Whether effectiveness is positive, negative, or neutral, each outcome shapes the next research stage when analyzing adoption rate drivers.

Appendix Three: Defining a Political Structure and the Role of Government

This study investigates critical relationships between the private and public sectors, which necessitates an understanding of "political structures" and the government's role. The study considers political structures a balanced relationship between two entities. In the US, this manifests as checks and balances between branches of the federal government. However, political structures may also extend to non-governmental organizations because policy affects both public and private groups. In the context of this study, a political structure refers to a balanced relationship between the public and private sector, and building this requires compromises from both sides. Just as checks and balances force a compromise in the law-making process, a stable political structure between private and public organizations requires each side to be willing to find a middle ground. The concept of balance is vital to a functioning political structure because if neither group compromises, progress becomes limited. In cybersecurity, the government needs to be willing to accommodate private firms' needs by streamlining requirements, and corporations must consider policy desires by investing in network defense.

The context of cybersecurity and achieving a balanced political relationship between private and public entities also requires an understanding of the government's role in securing private goods. This study demonstrates that the private sector is responsible for several critical infrastructure services that provide public goods – power, for example. Public goods are also the government's responsibility, and now that cyber capabilities can threaten these services, a balance between both groups is necessary. Although corporations are responsible for monitoring their networks, the government

must ensure that these defenses can stop dangerous adversaries. However, government mandates and requirements are not the answer to a balanced relationship, as American cybersecurity reforms demonstrated in the 2000s. Working relationships require policymakers to understand corporations' needs and create laws that help firms achieve political goals by providing them with resources instead of overbearing requirements. In exchange, the private sector must understand policy needs and be willing to work with the government to achieve broader strategic needs – in this case, building better cyber defenses. The study's recommendations follow these ideals and focus on creating tools or streamlined processes that can help firms secure their networks. Rather than creating mandates, which can result in decreased cooperation, the proposals attempt to make the government a supportive partner in cybersecurity to build a positive collaborative relationship with private organizations. The cybersecurity political structure balances public and private entities where compromise and cooperative dialogues are negotiation tools.

Bibliography

"Assessing Russian Activities and Intentions in Recent US Elections." Intelligence Community Assessment. Office of the Director of National Intelligence, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Barrachin, Marc, and Algirde Pipikaite. "We Need a Global Standard for Reporting Cyber Attacks." *Harvard Business Review, vol.* 592, no. 6 (November 6, 2019). pp. 1–5, https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks

Blank, Stephen. "Cyber War and Information War à La Russe." In Understanding Cyber Conflict: 14 Analogies, pp. 81–93. Georgetown University Press, 2017.

Boin, Arjen, and Allan McConnell. "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and The Need for Resilience." *Journal of Contingencies and Crisis Management* 15, no. 1 (2007): pp. 50-59. http://www.academia.edu/download/39525042/Preparing_for_Critical_Infrastructure_Br20151029-30676-1u12me.pdf

Caldwell, Tracey. "Spear-Phishing: How to Spot and Mitigate the Menace." *Computer Fraud & Security* 2013, no. 1 (January 2013): pp. 11–16. https://doi.org/10.1016/S1361-3723(13)70007-1.

Carlin, John P., and Garrett M. Graff. Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat. First edition. New York: Public Affairs, 2018.

Carr, Madeline. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, no. 1 (2016): 43-62. https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

Cartwright, James E (General, VCJCS). "Joint Terminology for Cyberspace Operations." Memorandum for Chiefs of The Military Services Commanders of The Combatant Commands Directors of The Joint Staff Directorates. Washington, DC: Joint Chiefs of Staff, November 2010. https://www.hsdl.org/?abstract&did=734860.

"CDM Program Overview." Washington, DC: Cybersecurity & Infrastructure Security Agency,https://www.cisa.gov/sites/default/files/publications/2020%2009%2003_CDM%20Program%20Overview_Fact%20Sheet_0.pdf.

Clément-Cottuz, Charlotte. "Risks in Governmental Cybersecurity Program: Case Study of the Einstein Project | Journal of Strategic Threat Intelligence." *Journal of Strategic Threat Intelligence* 1, no. 37 (November 2017): pg. 1–3.

Coats, Daniel. "Worldwide Threat Assessment of the US Intelligence Community." Office of the Director of National Intelligence, January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." Center for Naval Analyses, March 2017. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

"Cyber-Attack Against Ukrainian Critical Infrastructure." ICS Alert. ICS-CERT Alerts. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, August 23, 2018. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.

"Cyberspace Operations." Joint Publication 3-12. Joint Chiefs of Staff, June 8, 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

DHS.gov. "Critical Infrastructure Security." Department of Homeland Security. https://www.dhs.gov/topic/critical-infrastructure-security.

Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art." *Computer Networks* 44, no. 5 (2004): pp. 643-666. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.7118&rep=rep1&type=pdf

Dunn-Cavelty, Myriam and Manuel Suter, "Public–Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection* 2: 4, 2009, p. 181-190

"EINSTEIN | CISA." Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/einstein.

Etzioni, Amitai. "Cybersecurity in the Private Sector." Issues in Science and Technology 28, no. 1 (2011): pp. 58–62. https://doi.org/https://www.jstor.org/stable/43315569.

FEC.gov. "Campaign Finance Disbursements: Crowdstrike." Federal Election Commission. https://www.fec.gov/data/disbursements/.

"Framework for Improving Critical Infrastructure Cybersecurity." Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Gerasimov, Valery. "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations." Military Review 96, no. 1 (February 2016): pp. 23–29. https://doi.org/https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art001.pdf.

Gerovič, Slava. From Newspeak to Cyberspeak: A History of Soviet Cybernetics. Cambridge, Mass. London England: The MIT Press, 2004.

Giles, Keir. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power," March 21, 2016. https://www.chathamhouse.org/publication/russias-new-tools-confronting-west.

Harp, Derek R., and Bengt Gregory-Brown. "IT/OT Convergence: Bridging the Divide." White Paper. The SANS Institute and Nex Defense, 2014. https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf.

Hassanzadeh, Amin, Shimon Modi, and Shaan Mulchandani. "Towards Effective Security Control Assignment in the Industrial Internet of Things." In *2015 IEEE (Institute of Electrical and Electronics Engineers) 2nd World Forum on Internet of Things*, pp. 795-800, 2015. https://ieeexplore.ieee.org/abstract/document/7389155.

Heickero, Roland. "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations." Defense Analysis. FOI, Swedish Defense Research Agency, March 2010. http://www.highseclabs.com/data/foir2970.pdf.

"Heightened DDoS Threat Posed by Mirai and Other Botnets." Technical Alert. Washington, DC: Cybersecurity & Infrastructure Security Agency, October 14, 2016. https://us-cert.cisa.gov/ncas/alerts/TA16-288A.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." Lockheed Martin Corporation, January 2011. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

Jaikaran, Chris. "DHS's Cybersecurity Mission – An Overview." CRS Report. Congressional Research Service, December 19, 2018. https://fas.org/sgp/crs/homesec/IF10683.pdf.

Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H. Raghav. Rao, "Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear-Phishing Email," in *IEEE Transactions on Professional Communication*, vol. 55, no. 4, pp. 345-362, Dec. 2012, doi: 10.1109/TPC.2012.2208392.

Kattel, Ranier, and Ines Mergel. "Estonia's Digital Transformation." In Great Policy Successes, edited by Paul 't Hart and Mallory E. Compton, First edition., pg. 143–60. Oxford, United Kingdom ; New York, NY: Oxford University Press, 2019.

Knapp, Eric D., and Joel Thomas Langill. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress, 2014.

Kozlowki, Andrzej. "Comparative Analysis of Cyberattacks on Estonia, Georgia, and Kyrgyzstan." In International Scientific Forum, 3:236–45. Tirana, Albania: European Scientific Institute, 2013. https://www.researchgate.net/profile/Nnedinma_Umeokafor/publication/260107032_International_Scientific_Forum_ISF_2013vol3/links/02e7e52f964505c201000000.pdf#page=246.

Lee, Robert M., Michael J. Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid." Defense Use Case. Washington, DC: SANS-ICS and E-ISAC, March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Lesk, Michael. "The New Front Line: Estonia under Cyber Assault," in *IEEE Security & Privacy*, vol. 5, no. 4, pp. 76-79, July-Aug. 2007, doi: 10.1109/MSP.2007.98.

Lindsay, Jon R. "Stuxnet and the limits of cyber warfare." *Security Studies* 22, no. 3 (2013): pp. 365-404. https://doi.org/10.1080/09636412.2013.816122

Manpearl, Eric. "Securing US Election Systems: Designating US Election Systems as Critical Infrastructure and Instituting Election Security Reforms." *BU. Journal of Science. & Technology. L.* 24 (2018): pp. 168-192. https://www.bu.edu/jostl/files/2018/03/5-Manpearl-Online-Version.pdf

Ministry of Defense of the Russian Federation. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space) (Moscow, 2011). https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

Mueller, III, Robert S. "Report on The Investigation Into Russian Interference In The

2016 Presidential Election." Attorney Work Product. Washington, DC: US Department of Justice, March 2019. https://www.justice.gov/storage/report.pdf.

"National Cyber Strategy." Washington, DC: The White House, September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

"National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience." Washington, DC: Department of Homeland Security, 2013. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

Office of the President of Russia. "Greetings to Employees and Veterans of Russia's Energy Complex." Presidential Press Office, December 22, 2015. http://en.kremlin.ru/events/president/news/50991.

Office of the President of Russia. "Two New Power Units Connected to Russia's Power Grid." Presidential Press Office, December 22, 2015. http://en.kremlin.ru/events/president/news/50995.

Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Tallinn, Estonia: Cooperative Cyber Defense Centre of Excellence, July 2008. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

"Our Work with the DNC: Setting the Record Straight," June 5, 2020. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Parfomak, Paul, Richard Campbell, and Chris Jaikaran. "Cybersecurity for Energy Delivery Systems: DOE Programs." CRS Report. Congressional Research Service, August 28, 2017. https://crsreports.congress.gov/product/pdf/R/R44939.

"Preventing and Defending Against Cyber Attacks." Washington, DC: Department of Homeland Security, June 2011. p. 1-6. https://www.dhs.gov/xlibrary/assets/preventing-and-defending-against-cyber-attacks.pdf.

"Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies." ICS-CERT White Paper. Washington, DC: Department of Homeland Security, September 2016. https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf?force_isolation=true.

Rid, Thomas. Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Pub. L. No. 033017, § US Senate Select Committee on Intelligence, 1 (2017). https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf.

"Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." Joint Technical Alert. Department of Homeland Security: Cybersecurity and Infrastructure Security Agency, March 15, 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A.

Schmidt, Andreas. "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012." In The Estonian Cyberattacks, edited by Jason Healey. pg. 1-28 Vienna, VA: Cyber Conflict Studies Association, 2013.

Security Council of the Russian Federation. 2008. Доктрина информационной безопасности Российской Федерации. (Information Security Doctrine of the Russian Federation.) (Moscow, 2008). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

Security Council of the Russian Federation. Стратегия национальной безопасности Российской Федерации до 2020 года. (National Security Strategy to 2020) (Moscow, 2009). http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

Sergey Chekinov and S. A. Bogdanov, 'The Nature and Content of a New-Generation War,' *Military Thought*, No. 4, 2013., pp. 12-23. https://www.semanticscholar.org/paper/The-Nature-and-Content-of-a-New-Generation-War-Chekinov-Bogdanov/c8874593b1860de12fa40dadcae8e96861de8ebd.

Shackelford, Scott J., Michael Sulmeyer, Amanda N. Craig Deckard, Ben Buchanan, and Brian Micic. "From Russia with Love: Understanding the Russian Cyber Threat to US Critical Infrastructure and What to Do About It." *Nebraska. Law. Review.* 96 (2017). https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3118&context=nlr.

Singer, Peter W., and Allan Friedman. *Cybersecurity: What Everyone Needs to Know*. *Oxford University Press*, 2014.

Smith, Don C. "Enhancing Cybersecurity in the Energy Sector: A Critical Priority."

Journal of Energy & Natural Resources Law 36, no. 4 (October 2, 2018): pp. 373–80. https://doi.org/10.1080/02646811.2018.1516362.

Spitzner, Lance. "Applying Security Awareness to the Cyber Kill Chain." SANS Institute, May 31, 2019. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain.

Stauffer, Nancy W. "Protecting Our Energy Infrastructure from Cyberattack." *Energy Futures* 56, no. 2 (June 2019): pp. 1-8. http://news.mit.edu/2019/protecting-our-energy-infrastructure-from-cyberattack-0604.

Sullivan, Julia E., and Dmitriy Kamensky. "How Cyber-Attacks in Ukraine Show the Vulnerability of the US Power Grid." The Electricity Journal 30, no. 3 (April 2017): pp. 30–35. https://doi.org/10.1016/j.tej.2017.02.006.

"Supporting Policy and Doctrine | CISA." Accessed November 24, 2020. https://www.cisa.gov/supporting-policy-and-doctrine.

"The Cost of Malicious Cyber Activity to the U.S. Economy." Washington, DC: The Council of Economic Advisors, February 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

Whitehead, David E., Kevin Owens, Dennis Gammel, and Jess Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, 2017, pp. 1-8, doi: 10.1109/CPRE.2017.8090056.

Curriculum Vitae

Born on December 29, 1991, in Boston, MA, Christopher Yee-Paulson is currently a business development strategy lead at L3Harris Technologies. He is responsible for market analysis, business case development, and competitive intelligence at the firm's Washington DC Operations Headquarters since early 2020. From 2017 to the end of 2019, Mr. Yee-Paulson was a lead analyst with the Department of Defense (DoD) and responsible for strategic and technical analysis. During his time with the DoD, Mr. Yee-Paulson also served on the Joint Chiefs of Staff, providing analysis for senior policymakers, military officials, and flag officers. Before working for the DoD, Mr. Yee-Paulson was a senior analyst with Avascent, where he provided management consulting and data analytics services to major US defense prime contractors.

Mr. Yee-Paulson is a candidate for Johns Hopkins University's MA in Global Security Studies with a concentration in strategic studies – anticipated completion date December 2020. Mr. Yee-Paulson holds a BA in Political Science and Economics from Tufts University.